Deliverable 3:
Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens’ concerns and knowledge of stored personal data

Editor: Michael Friedewald, Fraunhofer ISI
Authors: Dara Hallinan, Michael Friedewald, Raphaël Gellert, Serge Gutwirth, Silvia Venier, Emilio Mordini, David Wright
Dissemination level: Public
Deliverable type: Report
Version: 1.0
Due date: 31 January 2012
Submission date: 16 May 2012
Terms of use

This document was developed within the PRESCIENT project (see http://www.prescient-project.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (co-ordinator),
- Trilateral Research Consulting LLP,
- Centre for Science, Society and Citizenship, and
- Vrije Universiteit Brussel

This document is intended to be an open specification and as such, its contents may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The PRESCIENT partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the PRESCIENT consortium. Address questions and comments to: coordinator@prescient-project.eu
## Contents

**Executive Summary**........................................................................................................................................ iv

1 **Introduction** ................................................................................................................................................. 1

2 **Citizens’ concerns and apprehensions about new technologies and their applications** .................................................. 3
  2.1 Introduction .................................................................................................................................................. 3
  2.2 Factors affecting public opinion .................................................................................................................... 4
  2.3 Citizens’ knowledge and concerns regarding data storage and use .......................................................... 11
  2.4 Conclusion ................................................................................................................................................ 19
  2.5 Outlook ...................................................................................................................................................... 20

3 **Citizens access to information: The data subject’s rights of access and information: a data controllers’ perspective** ................................................................. 21
  3.1 Methodological remarks ............................................................................................................................... 21
  3.2 The data subject’s right to information and of access to data .................................................................... 22
  3.3 The data subject’s right of access to data ................................................................................................... 39

4 **Assessment of DPAs activities on EU citizens access to personal data** ............................................................. 43
  4.1 Methodology ................................................................................................................................................ 43
  4.2 Data Protection Authorities (DPAs) in Europe ............................................................................................. 44
  4.3 Survey on how EU DPAs are handling citizens’ complaints ...................................................................... 51
  4.4 Conclusions ............................................................................................................................................. 90

5 **References** .................................................................................................................................................. 94

**Annexes** 99
A.1 Interview questionnaire template for Data Protection Authorities ............................................................... 99
A.2 Telephone Interviews with Data Protection Authorities ............................................................................... 101
A.3 Questionnaires received from EU Data Protection Authorities ............................................................... 102
Executive Summary

This report focuses on citizen perceptions, concerns and knowledge. Our analysis is carried with a view on three stakeholders:

(1) **Citizens**: The analysis of citizen perceptions is split into two parts. The first considers citizens’ concerns and apprehensions about new data collection technologies. The second considers citizens’ knowledge and concerns regarding data storage and use. The first section firstly considers the factors that shape public opinion on technologies. Then it considers the comprehension deficit in the conception of technologies giving a base from which to finally analyse fears.

(2) **Data Controller**: In this analysis we take a data controllers’ perspective on the data subjects’ right to be informed (article 10 and article 11 of Directive 95/46/EC), and the right of access to data (as enshrined in article 12 of the data protection Directive). To what extent can European citizens have access to the personal information and are they able to correct information and can find out how their information is being used?

(3) **Data Protection Authorities** (DPAs): What role do DPAs play in reconciling the rights and interests of data subjects and data controllers.

**CITIZENS’ CONCERNS AND APPREHENSIONS ABOUT NEW TECHNOLOGIES AND THEIR APPLICATIONS**

*Citizens’ concerns and apprehensions about new data collection technologies*

Perception of a technology is shaped by a number of factors. Firstly, demographic factors, such as the individual’s nationality, are significant, as are personal factors, such as the individual’s broader social tendencies and stance on issues related to a technology. Secondly, as the complexity of much new technology often leaves a knowledge discrepancy, second hand sources, such as the media, play a significant role in opinion formation. Thirdly, each technology conjures up images based on its presented operation, provoking greater or lesser reactions of unease. Fourthly, each technology is referenced to preceding technologies with opinion being shaped around common points of reference. Finally, the sphere of use (economic, social, etc.) will define the factors and mode of acceptance.

One significant trend in public opinion is the lack of solid understanding of many new technologies or the infrastructures in which they operate. Technological understanding is not always within reach of the general public and the environment of data flows, in which the risks manifest, is largely invisible to the individual. Thus the consequences of each technology are not necessarily easily comprehensible, or even directly relatable to that technology.

Thus, whilst there is an awareness of the potential and usefulness of data collection in certain situations, there is the uneasiness with which new data collection technologies are greeted. This is partly due to the lack of technological understanding but also due to the perception that the spread of technologies may be threatening to fundamental social principles. There is uncertainty about the legitimacy, reasoning and targeting behind
much data collection technology deployment. Unease also arises due to the complexity of related social issues, making tracing a path of causation between social debates and technological deployment difficult. In this sense, the public perceives data collection technologies as tools of power relations. Accordingly, the lack of identification and clarity as to the ‘who, the why and the how’ of the data controllers is seen as a significant concern, as is the potential for function creep or misuse.

**CITIZENS’ KNOWLEDGE AND CONCERNS REGARDING DATA STORAGE AND USE**

The consideration of citizens’ knowledge and concerns regarding data storage and use requires a deeper analysis than simply considering awareness of collected data forms. Accordingly, the section starts by considering knowledge of the current protection framework. It then considers public perception of the reality of the data environment before finally considering the logic of public engagement with this environment.

The public allocates data protection and privacy significant importance and the majority of Europeans are familiar with the framework’s key rights. However, knowledge levels drop considerably concerning the more abstract or complicated aspects of protection and the significance of data protection within a wider legal order. Although people are aware of the existence of the right to data protection, they are not immediately aware of why it has manifested as it has, nor have they considered its social function.

In the consideration of the data environment in reality, surveys demarcated key actors as state actors and private organisations. State actors were generally more trusted than private actors, while the level of trust also varied according to which state or private sector was considered. There is little conception as to the model of interaction between organisations, as to the flow of data between organisations or as to how allocation for responsibility for safe handling of data should be divided. It seemed that the public were particularly concerned about ID fraud, but also demonstrated concern and annoyance at the commercial collection and use of data. Although the public also expressed more abstract fears related to the social implications of data assemblages, these were at best only loosely defined.

Despite the fact that 63% state that disclosing personal information is a big issue for them, individuals seem to accept the need to divulge increasing amounts. This is based on the deterministic viewpoint that disclosure is ‘simply part of modern life’. Firstly, there is the perceived obligation, legally and practically, to release ever more information. Secondly, the public recognise short and long term benefits from disclosure – in the form of exchanges for rewards and participation in data environments. There is thus a considerable difference between abstract opinion and concrete behaviour.

It is clear that the public comprehend neither the supporting technological infrastructure nor the data flows and networks that make up the data environment. Thus, whilst not unaware of dangers and the existence of structures through which data processing and protection operate, there is a lack of understanding as to how and why they operate. This limits the ability of the individual to rationally balance each transaction for benefits and consequences. This provides little basis for practical and considered decision making in an environment in which increasing data disclosure is perceived as a necessity for everyday life and for participation in society in general.
THE DATA SUBJECT’S RIGHTS OF ACCESS AND INFORMATION: A DATA CONTROLLERS’ PERSPECTIVE

We have examined the website of some of the most important data controllers (namely, Google, Microsoft, Facebook, Wikimedia, Amazon), and assessed the extent to which the information disclosed in the privacy notices is in line with the requirements of articles 10 and 11 of the data protection Directive. In particular, we assessed them against the test constituted by Opinion 2/2001 of the Article 29 Data Protection Working Party (Art 29 WP) on certain minimum requirements for collecting personal data on-line in the European Union, and opinion 10/2004 on “More Harmonised Information Provisions”. We also used the recent letter that the CNIL (French DPA) addressed Google regarding the conformity of its new online privacy notice with regards to the aforementioned Opinions, and which provides guidelines as to the substantive quality of the information provided.

Some consistent trends emerge from such analysis. There are persistent misconceptions as to the meaning of personal data, as several data controllers take a very narrow view and consider as personal data only the information that users have voluntarily disclosed. In general data controllers are quite elusive as to the duration and purpose(s) of the processing. Many shortcomings have been also observed as to the information provided concerning the right of access to data. These several shortcomings can be understood and analysed in the light of the substantial requirements concerning the information provided that are to be found in the CNIL’s letter to Google. Furthermore, issues of applicable law to the data controllers might (at least) partly account for some of the shortcomings observed. Finally, it is worthwhile observing that many data controllers have adopted multi-layered privacy notices in the wake of the Art 29 WP’s opinion 10/2004 on “More Harmonised Information Provisions”. Yet, such a simplification of the explanatory framework should not be undertaken at the expense of the quality of the information provided.

In a second part, we aimed at determining how data subjects concretely exercise their right of access (if at all) from the perspective of data controllers, that is, how do data controllers experience users’ demands of access to their personal data. To this end, we have contacted data controllers and asked them a list of question concerning the data subject’s right to access. This exercise proved to be more difficult than anticipated. In the first instance it proved extremely difficult to reach, be it trough phone, e-mail, or regular physical mail, a responsible person who had competences to address such requests. Second, even in cases where we managed to find the responsible person, either no information was available; either the data controllers were not in a position to gather evidence in order to answer our questions.

ASSESSMENT OF DPAS ACTIVITIES AND SELECTED STAKEHOLDERS OPINIONS ON EU CITIZENS ACCESS TO PERSONAL DATA

Within the scope of PRESCIENT WP3, the aims of task T3.2 are to analyse the attitudes towards data protection issues of the main data controllers in Europe (part 1), and to assess to what extent EU citizens are notifying violations of data protection rules to the competent authorities and how these institutions are reacting to these claims (part 2).
The research conducted in the scope of T3.2/Part 2 has been carried out in 2 main phases. The first step was the analysis of the websites of the Data Protection Authorities of the 27 Member States and the European Data Protection Supervisor as well as the Art. 29 Working Party (DPAs websites inspections). The second step was to prepare a questionnaire and to send it to all Data Protection Authorities in Europe in order to collect more information on their activities (interviews). The purpose of the questionnaire was to gather contributions from DPAs in Europe on citizens’ attitudes towards data protection, to assess to what extent EU citizens contact European DPAs and how these institutions are reacting to and supporting these claims. This touched both the question of how individual data subjects or groups of data subjects are asserting their rights as well as on the more general question of whether supervisory authorities are willing and capable to enforce the law. We proposed the questionnaire to all Data Protection Authorities in Europe, as well as to the European Data Protection Supervisor. Out of 27 Member States and 1 EU institution (EDPS), 19 Authorities replied to the questionnaire.

The first part of the questionnaire (Q1-Q4) was an assessment of the structure and independence as well as of the competencies of the national DPAs. With respect to the DPAs’ independence, there is a great variation across Europe that mainly depends on the national legal framework through which the authority was established. With particular respect to the competencies of the national DPAs, in general these include: to advise the legislator in the process of drafting legislation or regulations relating to the protection of the individual’s rights and freedoms with regard to the processing of personal data; to create and maintain a public register of all processing operations being notified by data controllers, in order to facilitate access to information for the data subject; to deliver prior-checking opinions before processing operations are carried out; to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller; to institute civil legal proceedings in cases where the provisions of the national data protection act have been or are about to be violated; to encourage the drawing up of suitable codes of conduct by the various sectors and to provide a data protection audit; to raise public awareness on matters of data protection and privacy; to collaborate with supervisory authorities of other countries or at the EU and international level to the extent necessary for the performance of their duties. European DPAs are often confronted with the problem of limited resources to carry out their tasks. The lack of financial and human resources is often indicated as a major reason preventing the DPA to accomplish its duties. In the questionnaire, particular attention was devoted to assess EU DPAs awareness-raising activities. According to many respondents, as a consequence of an increased effort in public awareness campaigns in recent years, the DPAs are experiencing a significant increase in the requests of information, as well as in the submission of notifications and complaints.

The second part of the questionnaire (Q5-Q10) was particularly devoted to analysing how DPAs are handling citizens complaints. In all European Union Member States, citizens have the right to request an investigation on the grounds of infringements of the data protection law. The study showed that the DPAs are noticing an evolution in the number and type of complaints received. For many years, the number of complaints was quite stable and relatively low, but in the last decade there has been an increase. Citizens usually address the DPA to pose questions on their rights in a specific case, to request...
assistance to access/rectify/delete information, and to report violation of data protection rules. There is an increasing trend in complaints related to data processing in online services. Other sectors mainly include video surveillance in public spaces, surveillance at work, as well as data processing in the public health and financial sectors. With reference to the ability of the DPA to react on time to citizens’ claims, the time to handle a claim may vary a lot depending on the nature of the complaint. In easy situations, a letter to the data controller might resolve the problem in a week. When the complaint need to be verified in order to collect evidence, this may require an inspection. Some delays may also occur also when the DPA has to wait for information on data processing from a public institution, a private company, or the DPA of another country.

The last part of the questionnaire (Q11-Q13) was devoted to collecting DPAs perceptions on the recently proposed reform of EU data protection legal framework. A few DPAs replied that it is still too early to comment on this, that they are in the lobbying and analysing phase. According to other DPAs, some positive impacts may be already noticed, above all in the joint work carried out in the scope of the Art 29 WP, as well as the case-handling workshops, and the cooperation with joint supervisory authorities in the field of enforcement (e.g. exchanges of information, joint measures, joint inspections), and with DPAs in other countries. Co-ordination and co-operation mechanisms have been already in place since 1995, but they are expected to be strengthened through the new rules, both in the law enforcement field and in relation to the work of the European Data Protection Board and in particular of its activity with regard the “consistency mechanism”. With regard to the expected positive outcomes of the new data protection reform, in the respondents’ view the reform will strengthen the rights of individuals in terms of increased transparency, greater control over processing, data minimisation, specific provisions for processing of children’s personal data, strengthened data access rights, the right to object, the right to data portability, and the right to data deletion (“right to be forgotten”) and strengthened rights of redress. The obligation for large companies to have a data protection officer (DPO), who will be responsible for dealing with the DPA, was also mentioned as a positive outcome of the reform.
1 Introduction

The first PRESCIENT deliverable examined the legal, social, economic and ethical conceptualisations of privacy and data protection and made general suggestions about how both privacy and data protection might be challenged by new and emerging technologies, particularly in relation to ICT and surveillance technologies.\(^1\) The second PRESCIENT deliverable analysed specific emerging technologies posing challenges to privacy and data protection. In particular we identified uncertainties and inadequacies in the legal environment as a result of these technologies.\(^2\)

In this third deliverable we now focus on citizens, and their concerns and knowledge regarding privacy, data protection and new technologies and on their access to their personal data.

The main aims of this report are:

1. To determine whether European citizens have sufficient knowledge of what information is stored, for which purpose and for what period of time.
2. To assess how easy or difficult it is for European citizens to have access to information that is stored about them and to correct such information.
3. To collect and assess the views of a representative sample of data controllers with regard to privacy and data protection and, in particular, whether they view transparency – for individuals seeking knowledge of their data – as being in data controllers’ own interest.

In chapter 2 we assess citizens’ knowledge of what information is stored, for which purpose and for what period of time. To do this, we analysed existing surveys and analyses through a systematic review process and conducted a meta-analysis of their results in order to evaluate the strengths and weaknesses of citizens’ current knowledge about data protection and privacy. Whilst it turns out that there are many public opinion polls on citizens’ attitudes towards privacy or data protection, these often contain significant bias or methodological weaknesses and only seldom cover citizens’ concerns and apprehensions about specific new technologies and their applications. The chapter is split into two parts. The first considers citizens’ concerns and apprehensions about new data collection technologies. The second considers citizens’ knowledge and concerns regarding data storage and use.

Chapters 3 and 4 are devoted to analysing to what extent European citizens are aware of the amount of personal information that is shared and processed about them, and to what extent they are able to access and correct their data. Our aims are to analyse the attitudes of the main data controllers in Europe towards data protection issues, and to assess to what extent EU citizens are notifying violations of data protection rules to the competent authorities and how these authorities are reacting to these claims.

---


Chapter 3 takes a data controller’s perspective on the data subject’s right to be informed and on the subject’s right of access to data. It addresses the question as to the extent to which European citizens have access to the personal information that is collected, stored and processed, if they are able to correct this information and if they can find out how their information is being used. For this purpose we examine the websites of five of the most important data controllers and assess the extent to which the information given in their privacy notices is in line with the requirements of the Data Protection Directive. In a second step, we aim at determining how data subjects concretely exercise their right of access (if at all) from the perspective of data controllers, namely, how do data controllers experience users’ demands of access to their personal data.

Finally, chapter 4 aims at assessing to what extent European citizens are contacting Data Protection Authorities (DPAs) in their Member States to complain about difficulties in accessing their personal information or about other violations of data protection law, as well as at assessing how the supervisory authorities are handling citizens’ complaints. The study also resulted in an analysis of the structure and competencies of DPAs at national level, as well as an analysis of DPAs’ perspectives on the recently proposed amendments to the EU data protection legal framework, in relation both to their capacity to hear citizens’ claims and to enforce the law. This was done through a survey and additional interviews with representatives of European DPAs.
2 Citizens’ concerns and apprehensions about new technologies and their applications

Dara Hallinan, Michael Friedewald (Fraunhofer ISI)
David Wright (Trilateral Research and Consulting)

2.1 INTRODUCTION

There is an increasingly broad range of technology collecting and processing data. This technology is deployed in different scenarios depending on its technological specificity and the development of its use. Increasingly, the privacy impacting effects do not stem from each individual technology; rather, the technologies facilitate the collection of different types of information. The impact then arises when specific technologies are combined with information processing capabilities, allowing the combination of previously diverse sources of information, the linkage of collected data with existing pools of data and broader significance extraction capabilities from multiple sources.

Citizens’ concerns and apprehensions arise from a wider process of opinion formation in which a number of factors play a role. In order to comprehend and categorise not only fears, but also the driving forces behind these fears, the logic of their manifestation and their relation to other aspects of public opinion on data collection and processing technologies, a holistic view of the process and factors involved in public perception of new technologies must be taken before considering fears specifically.

Accordingly, this section will firstly consider the factors that shape public opinion on technologies. Then it will consider the comprehension deficit often present in the conception of technologies and where this may have come from. This will provide a base from which to finally conduct a substantial analysis of the content and nature of resultant fears.

As in the case of data protection and privacy issues generally, information relating to public opinion on new data collection technologies is difficult to evaluate as there have been few related surveys. Perhaps this is because the issue of data collection as it currently manifests and the technologies now significant in the field have only recently entered public consciousness, or perhaps it is because the data environment, as a relatively abstract concept (particularly in relation to data assemblages), is not a theme easily associated with public opinion. Equally, many of the surveys that have been conducted have been from the American perspective. This may significantly prejudice the use of their findings when considering the EU public.

---

3 For an overview, see Petersen, Julie K., Understanding surveillance technologies: Spy devices, privacy, history and applications, Auerbach Publications, Boca Raton, 2007.
2.2 FACTORS AFFECTING PUBLIC OPINION

For a variety of reasons, there is no single ‘public opinion’ on new technologies. Due to their varying contexts, capabilities, visibility, effect and comprehension, opinion can vary greatly. However it is possible to isolate certain more general factors which appear key to the shaping of opinion. These come together (balanced differently dependant on context) to chart a background to each perception.

A range of demographic qualities plays a role (age and gender demand mention). Amongst these, nationality and national culture are specifically important. As Samatas clarifies in the Greek context regarding surveillance, the history and cultural background of a state has specific relevance in relation to the consideration of data collection. This defines a series of further issues and consequently defines the borders within which the further specifics of a technology will be received. An example of this is the lack of the tradition of ID cards in the UK and the significant resistance their mooted introduction has encountered. Another example is the differences in survey responses between Northern Ireland and those in Great Britain regarding CCTV (considering its historical and authoritarian connotations in public use and its perceived lack of necessity in private use). This was also the finding in the PRISE project, where debates over the deployment of new security technologies were deeply linked to debates over national public morals.

Also of importance is the individual’s current (and past) stance on matters relevant to a given technology. For example, should an individual feel particularly strongly about the issue of data protection, it is unlikely they will greet the broad introduction of biometric ID cards favourably. Related to this will be an individual’s broader social tendencies. For example, as Murphy points out, public perception of the privacy vs. security debate can be broken into three groups who share similar characteristics. In the more authoritarian group, respect and trust for authority and the prioritisation of security over other social goals is a key feature. Thus, we can assume that members of this group would respond more favourably to deployed surveillance technologies than those of another group in which these traits were less prevalent.

---


A significant body of information regarding the use and operation of this new technology will often be second-hand. In this respect it is enlightening to consider the number of real encounters with new security technologies (for example, in an Opinion Research Corporation survey in the US from 2002 it was found that only 5% of respondents had actually provided biometric characteristics that year). Whilst specific evidence is scarce, a picture begins to form when considering the more in-depth interview answers in the PRISE project, for instance, where opinions on technologies became increasingly theoretical and anecdotal as the novelty of the technology increased. The prevalence of personal damage felt as a result of the use of these technologies may also be relatively small. Thus, sources such as the media will play a significant role in the building of conceptions of technology, its operation and the tone of opinion. Many of these sources have their own internal logic and founding positions and as such the consideration of the consequences, problems and operation of a technology will rarely be presented objectively and presentation will often be situated within other, broader, debates. Indeed, significant and relevant knowledge, awareness and factual understanding can often be obscured by this merging of debates and the hidden, or background, logic of the sources involved in creating the opinion discourse. For example, the striking, easily identifiable term, “naked scanner” comes with a series of background connotations and its use conveys strong emotional imagery which can immediately damage the public view of the technology.

Each technology also conjures up images based on its presented operation. Firstly, certain of these images may provoke more immediate reactions of unease than others. For example, retinal and iris scanning may be received differently from other forms of biometric partially as they are seen to be focussed on a particularly fragile and vital area of the body while the obvious impact of the body scanner, or ‘naked machine’, immediately conjures negative images of blunt tangible bodily privacy invasion. The PRISE project specifically points out a high resistance to “physically intimate technologies”. Secondly, the public reference each technology to preceding technologies. When there are a greater number of reference points for the operation and effect of a technology, its reception will be predicated on these references. For example, public opinion formation around fingerprinting as a biometric is subject to a different set of considerations compared to other biometrics as the concept of fingerprinting has a significant history of use as a unique identifier. The public thus view the technology differently from other technologies. The same is true of the location, logic and action of use. The more the public can associate with, and establish precedent for use in a context, the more solid opinion formation will be.

---


The economic, social (or other) space of use of a proposed technology will also influence its public acceptance. Backhouse comments on the acceptance of technologies used by the state as being based not only on systemic reference points, but also public feeling as to the “trustworthiness” of the operating institutions. Significant factors in this regard are existing perceptions of levels of competence, benevolence and integrity each institution and structure has. In the economic context, while the same factors are taken into account in relation to the levels of trust and “trustworthiness” of an industry or organisation, these are accompanied by a further series of considerations equating to a cost-benefit analysis of the use and acceptance of the new technology – the “privacy calculus”. In this calculus, the public will consider whether a technology embodies expectations of procedural and distributional fairness in operation.

### 2.2.1 Public opinion lacks technological understanding

The range of new data collection technologies and the difference in their operation makes it difficult to pinpoint universal attitudes. However, certain trends and factors in current opinion can be isolated. Perhaps the most significant of these is that the public has little solid understanding of many new technologies or their operation. Public understanding of a technology comes about through a series of reference creations which build a body of comprehension, placing the technology more solidly within broader conceptions. The novelty of technology (at least in the public mind) and the complexity of its operation and effects often mean this process is currently in a state of flux. In essence, the public still lacks the metaphors through which to view these technologies. Hence, the critical features and impacts at each individual and social level are subject to uncertainties which, refracted through the above features influencing perception, may paint a significantly distorted picture.

The technological understanding of new data collection technologies such as RFID or biometrics is not always within reach of the general public. This is not to say its comprehension is impossible (at least comprehension of the relevant activity even if not of the technical specifics), simply that this information is often not presented by sources presenting opinion forming information. As a consequence, the public’s comprehension of the function, capability and the inherent danger in each technology derives from other references (or sometimes not at all). The public perception of terminology is often significantly confused. Terms for families of technologies are sometimes presented by public information sources, and thus viewed by the public, as one technology. Judging from uncertainty in other aspects of perception, we can assume

---


15 Webster, William, "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance and Society*, Vol. 6, No. 1, 2009, pp. 10-22. This article considers the observation that the public knows little about CCTV in terms of its operation but that as a result of widespread media coverage, interest in the technology is growing. Some have suggested that this lack of understanding and knowledge about the actual impact of CCTV on crime and other anti-social behaviour is a key factor in high levels of support for CCTV amongst some groups.
that the public thus is not always aware of exactly what is being discussed.\textsuperscript{16} For example, the term biometrics does not describe one single technology but rather is an overarching description for a series of identification technologies, including second generation behavioural identifiers. Each of these differs significantly from the others in use, capability, privacy impact and technology with significant practical consequences depending on context.\textsuperscript{17}

The consequences and important impacts of many new technologies come not in their isolated use (although some technologies such as body scanners have a more visceral and obvious privacy impact), but in their combination with other technologies or systems. For example, there is a significantly reduced privacy risk in 1:1 systems than with 1:N systems connected to central, or even multiple, databases ("a system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system. A 1:N biometric system would be necessary for use in any indiscriminate large-scale searches" \textsuperscript{18} whilst a 1:1 system would be used for simpler verification purposes). It is often the consequent data processing operations, which are not part of the technologies themselves, which create the critical privacy impacts. The problem is that the environment in which the risks manifest is incredibly complicated and largely invisible to the individual and the consequences of each technology are not necessarily easily, or directly relatable to that technology. Thus, when risks are presented on any level, from the individual to the social, there is a lack of clarity as to how they relate to any specific technology.\textsuperscript{19}

It is technology, its deployment and combination (as well as its combination with data processing capabilities) that provides the foundation for the development of surveillance in modern society. However, the lack of clarity in comprehension or perception of technology means the public is often left making presumptions about the significance and capability of its operation (both as it stands alone and as part of a wider infrastructure).\textsuperscript{20} This provides a poor basis for the formation of a picture either of the


\textsuperscript{20} In considering the difficulty the public has in percieving the online data environment, it is useful to consider the data environement as consisting of two parts: supporting technological infrastructure (and its innate capabilities) and the operation of the network of data connections and flows (see section 2.3.5 below) In each consideration of technology, the public showed a significant lack of awareness as to the capabilities, uses and key privacy impacting features present, demonstrated well in the U.S. survey; ibid. A lack of understanding as to the shape and operation of the data flows themselves is demonstrated in Brandtzaeg, Petter Bae, and Marika Lüders, "Privacy 2.0: personal and consumer protection in the new media reality", Norwegian Consumer Commission, Oslo, 2009. http://forbrukerportalen.no/filearchive/report_privacy_social_media_1_.pdf
nature of technology within a data environment, the significance of the data it collects and its significance against a wider social background.

2.2.2 Fears

Whilst there is an awareness of the potential and usefulness of data collection in certain situations (particularly in recognised security hotspots or for the ease of use of certain services), there is the uneasiness with which new data collection technologies are considered and greeted even as they purport to answer supposedly desired social/individual needs such as the fight against terrorism. This is partly due to the public’s lack of technological understanding but it is also due to the awareness that the proliferation and perceived deterministic use of technologies may be creating something more sinister and potentially threatening to fundamental social principles (indeed a certain PRISE minority stated they would not accept biometrics under any circumstances).

There is further uncertainty about the reasoning and targeting behind much data collection technology and the logic, honesty and legitimacy according to which it is alleged to achieve its stated ends (70 per cent of respondents did not believe technology was effective against terrorism but that it was deployed to create the appearance of action – “security theatre”, as Bruce Schneier calls it). The logic of technology at the expense of other potential solutions (such as tackling causes) is questioned as are certain other assumptions of deployment, such as that a violation of privacy without significant proof of intent is justified (this is not always an assumption, but in certain surveillance technologies, there is a necessary relinquishment of privacy without the necessity for any intent to be demonstrated). Uncertainty arises partially due to the complexity and breadth of the related social issues and the difficulty in tracing a path of causation in social debates and technological deployment and partially as the technologies are seen to have widespread potential outside their designated deployment.

purposes (function creep).\textsuperscript{26} Function creep makes some people wary about taking data collection related steps, as they feel that once a technology is deployed it will be difficult (even impossible) to ever remove it while the strength of limitation on function is often difficult to discern. The perception of the non-transparent development of a consequential data infrastructure is present in the public imagination.\textsuperscript{27}

In a broad sense, the public appears to perceive data collection technologies as technologies of power relations. Indeed, people do not directly disapprove of the technologies themselves: it is the feeling of being “under observation” (in security terms, “under suspicion”) that they engender on the part of the observed which appears to be of key concern.\textsuperscript{28} Perhaps considering the confusion in the logic of deployment and networks of relations, it is a common theme that the lack of identification and clarity as to the “who, the why and the how” of the data controllers is seen as a significant concern (the reality and proximity of this fear is closely tied to levels of trust). This can be assumed to represent an abstract appreciation for the ability of these technologies to reshape the individual’s place and therefore by extension, key relationships and concepts, within society. However, the theoretical awareness of possibility does not seem to stretch to a more elaborated perception as to how this might happen.\textsuperscript{29}

At an individual level, general data processing fears are transferred onto the background of each new technology, with respondents listing concerns such as the occurrence of ID fraud, function creep, secondary use and misuse.\textsuperscript{30} This finding also came through in the PRISE project, as in each of the six countries surveyed, there was a strong conviction that security technologies would be abused (function creep, misuse) and create direct personal effects. It is indicative of the apparent gap in understanding of individual technologies as opposed to their presence in wider infrastructures or as part of wider debates, that the precise manifestation of these effects, or fears specifically related to one technology, rarely arose without prompting.

\textbf{2.2.3 Conclusion}

When considered alone or as part of wider assemblages, it is evident that the technical capabilities of data collection technologies are not often understood, whilst in their presentation, the terminology is mixed and uncertain and the boundaries of discourse around and between technologies are fluid. As a consequence, the public has difficulty in
forming images of the technologies themselves or of locating the significance of the data they collect, the data environment they operate in or their relevance in wider and equally complex social debates. It is thus very difficult for the public to evaluate technologies themselves or the wider systems of which they are part, based on relevant factual starting points.

As a result of this lack of clarity, other opinion-shaping factors become significant in whether technology is accepted and the role it plays in wider debates (such as how technologies are presented in the media or the immediate reaction they elicit). Whilst the technologies and the systems in which they operate are active features in the significance of data collection and processing, it is, in fact, their references in relation to other debates or perceptions that play the active role in public opinion formation.

Accordingly, considering the lack of comprehension of the technologies themselves and therefore a difficulty in tracing paths of causation between their deployment and use, and their justification, consequence and legitimacy related to their declared aims as well as related to the social systems with which they interact, public fears took on two forms. First, uncertainty led to a general feeling of uneasiness related to the increased deployment of data collection technologies and what the trend toward increasing collection of personal data could be fostering, both on a societal level, and in terms of what this would mean for the individual in society. The individual manifestation of this uncertainty was perhaps personified best by the indefinable but uncomfortable expression of feeling under suspicion. Second, specific manifestations of abstract fears, guided and filtered through the above mentioned opinion formation factors, thus tended to be transferred onto each technology, with fears of ID fraud, function creep, secondary use and misuse being particularly prevalent.

2.2.4 Outlook

From the above, one can identify certain public desires in relation to data collection technologies. First, the public wish the lack of knowledge and certainty about data collection technologies – what they are and how they are to be used – to be addressed.

Second, the public has the perception that there is little debate on the theme and on why, which and how to deploy each technology, and that policy makers should address this too. As it is perceived that the effects of technological deployment could be socially significant there should be wider debate on technological deployment and use. These debates should also include consideration of non-technological solutions and should include a wider range of stakeholders in the decision making process.

Before the deployment of each technology, to reduce the potential for function creep and privacy impact, the public believe that the privacy impact should be carefully analysed and considered against potential gains.31

Finally, there should be further transparency and controls on the operation and use of each technology. This can be seen as a reflection of the perceived need for control over

the social impact of the technology, the consequences of its wider deployment and the potential for function creep and misuse.32

2.3 CITIZENS’ KNOWLEDGE AND CONCERNS REGARDING DATA STORAGE AND USE

2.3.1 Introduction

The consideration as to whether the public knows what data is stored, why and for what period requires a deeper analysis than simply a consideration of awareness of collected data forms. This is not only as a simple gathering of opinion on what individuals believe is stored would yield relatively little of normative or novel value, but also as the reduction of data collection to the specifics of information collected obscures the critical connections and networks (both social and technical) out of which the data environment is created and through which data collection impacts and interacts with each citizen.

Accordingly, the consideration of citizens’ knowledge of data collection, storage and use is a consideration of citizens’ perceptions of the connections and purposes behind the development of the data environment and their place within and interaction with this environment. This environment can be considered as being made up of two parts. First, there is the regulatory framework which defines the rules of the environment and its supposed theoretical place and interaction with other aspects of society, and second, there are the networks and flows of data which construct the environment proper. Citizens’ perception of each of these parts, how they interact with each other and how each citizen conceives of their role in relation to these parts must all be considered to create a holistic model of knowledge and concern regarding data storage and use.

Accordingly, after considering the range of publics observed in the various surveys, this section takes as its starting point public awareness and knowledge of the current data protection framework as the template for the regulation of data collection and flows and as the key framework safeguarding citizens’ rights in the data environment. This will provide an impression of awareness and perception of the theoretical basis of data protection as a system itself and within a wider system of law.

Following this, the section will consider public perception of the data environment in reality, considering who the public believes to be the key actors in data collection and processing and what their opinion of them is, where responsibility within this environment should be allocated and which fears related to processing commonly arise.

The section will then attempt to add depth to the causes and logic of public engagement with the data environment, especially considering the uncertainty and inconsistency which arises out of public knowledge and concern and yet the lack of practical or behavioural evidence demonstrating this concern.

32 Ibid.
Finally, the section will consider how effective the public perceive the regulatory framework to be against the reality of the data environment, and will offer some indication of where the public feels the weak points of the framework to be.

2.3.2 There is more than one “public”

The European public is a diverse body in which an enormous range of views and perspectives are present. A range of factors can have an effect on perceptions and approaches toward data protection and privacy such as social status, political affiliation, income, education, profession and gender. The correlations of these factors to a specific set of perceptions can be very difficult to pick apart and each factor may play a greater or lesser role in relation to each issue.

Particularly significant appear to be nationality (and consequently national culture) and age (or more precisely familiarity with the digital environment). The differences between national results in surveys can be considerable. In Eurobarometer 359, for example, knowledge of the national Data Protection Authority varied from 51% in Hungary to just 16% in Spain. An expansion of this even reveals broader regional trends (for example, a Scandinavian group perspective can be isolated). In the same survey, there is a specific separation and investigation into the specifics of digital natives and initiates (those who were born and raised with, or subsequently became familiar with, digital technology) and other, predominantly older, respondents.

Even when a viewpoint appears to be identifiable, the complexity of the issues involved means this is never monolithic and, considering the fluidity of understanding in relation to the technical and social background to each view, may be subject to qualification or change dependant on context of application or to circumstantial change.

2.3.3 What does the public know about the current protection framework?

Survey results make clear that the public attaches significant importance to data protection and privacy. Indeed, in the "Public Awareness Survey 2008" carried out on behalf of the Irish Data Protection Commissioner, the privacy of personal information was ranked third in order of importance (with 84% regarding it as “very important”) in a list of key issues, trailing crime prevention by only 3%.

Whilst there seems to be a considerable variation between citizens in different European countries in relation to their knowledge of protection frameworks and the

---

protections they offer, the majority of Europeans appear familiar with the key rights the data protection framework offers. For example, although a citizen’s right to access data held by others’ was the least known amongst respondents, the EU awareness average still sat at 59%. However, knowledge levels dropped when respondents were questioned as to the more subtle, abstract or complicated aspects of protection, such as the status of sensitive data or the situation relating to cross-border data flows. More minor sectoral or supporting legislation made no appearance in any survey, nor were they brought up spontaneously by any lay respondent.

There is not the same level of awareness regarding National Data Protection Authorities (NDPAs). In the same Eurobarometer, the EU average awareness of the existence of NDPAs sat at a low 28%. Amongst those aware of the existence of local NDPAs, there was still considerable uncertainty as to their remit and capability (e.g., whether they could impose sanctions). Although this may be partially explicable, assuming an individual who has not had cause to complain may not be expected to have found out about a national authority, these figures do not align with knowledge of aspects of protection. This suggests an imbalance in awareness between the letter of protection and its operation in fact.

The status of data protection within the contexts of a wider legal order was rarely mentioned or apparently considered. This is to be expected, not only as its elevation to the status of fundamental right has only been recent and through an instrument and means which may themselves not be so transparent or apparent to the individual citizen but also as the significance and consequences, both theoretically and practically, are still uncertain. On the other hand, one would expect a high understanding of fundamental rights. Public lack of awareness of the right to data protection is incongruent with this.

The above point brings into question how citizens view and understand privacy and data protection within a wider system of law and society. Although people are aware of the existence of rights, they are not immediately aware of why they have manifested as they have, nor do they appear to have given much thought as to their social function. However, when longer discussions ensued considering wider erosions of privacy and potential threats to, and arising from, personal data processing, participants began to voice fears based on the social dimensions of the rights, although they often found these difficult to elaborate and articulate. This perhaps demonstrates an imbalance in the public’s concepts of privacy and data protection in relation to its dual individual and social functions. This resonates with Solove’s commentary: “Privacy is often cast as an individual right and balanced against the greater social good, which results in privacy being frequently undervalued.” There are factors which mediate toward making this so. First, it is not high on an individual’s list of priorities to consider the social conception of any right, let alone rights as complicated and abstract as data protection and privacy. Second, the invisible and unknown environment in which data protection issues play out (we will return to this point) may make it difficult for the individual to conceive of social impacts, social importance or trace the consequences of aggregate action in a considered way. Finally, the public’s reference points for data protection are

37 Ibid.
percieved as revolving around individual actions (for example, a purchase while shopping online)\textsuperscript{39} and single trade-offs, as opposed to actions with systemic significance or involvement in issues which may have social significance.

\subsection*{2.3.4 Public view of the regulatory environment}

\subsubsection*{2.3.4.1 Actors}

Surveys generally distinguish between state actors and private organisations (normally companies). "other individuals", whilst mentioned tangentially in relation to other questions (ID theft, for example), were not isolated as important actors in the surveys considered. This is particularly interesting considering the key role played by the individual in the online environment and the individual nature of many perceived threats. Within this differentiation, state actors tended to be (often considerably) more trusted than private actors. This was broken down further to show that certain state sectors were trusted more than others. For example, in Flash Eurobarometer 225\textsuperscript{40}, medical services were highly trusted with an 82\% positive trust rating, whereas local authorities scored a lower 67\%. However, these numbers obscure a more nuanced understanding of the issue. When the public is further questioned on the issue of trust in state institutions, whilst there seems to be a belief that institutions will try to behave in the right way, there is a far lower belief in their capability to control and safeguard the data they have been given. This could be at least partly as a result of constant media coverage relating to authorities' leakage of personal data.\textsuperscript{41}

Within the private sphere, there is also considerable trust variation. In the same Eurobarometer survey, banks received a 66\% trust rating (although perhaps this would be different now in 2012), whilst mail order companies received a trust rating of only 24\%.\textsuperscript{42} However, despite these statistics, when deeper opinion was sought regarding commercial organisations' handling of personal data, a distinct undercurrent of distrust emerged. Whilst respondents predominantly disapproved of sharing between government and private organisations, Eurobarometer provided little elaboration as to what the public believed was the model of interaction between organisations, or as to the flow of data between organisations. In essence, there was little elaboration of a model beyond the superficial first instance of data collection.

\subsubsection*{2.3.4.2 Responsibility allocation}

Generally, the public does not seem certain which actors should be responsible for the safe handling of personal data. Indeed, opinion changes depending on the nature of

\begin{thebibliography}{99}
\end{thebibliography}
entity or activity considered. When considering social networking sites, for example, 49% of respondents stated the individual should be primarily responsible with 33% suggesting the social network should be responsible, whilst in relation to online shopping sites, the percentages were 41% and 39% respectively. The difference is interesting not only as it demonstrates uncertainty in responsibility allocation but also as it suggests a difference in perception based on the nature of the specific data processing entity. Taking this logic one step further suggests the public may be basing its opinions more on the entity than on the processing of data. Equally interesting is the relatively low response listing public authorities as having primary responsibility (16% and 19% respectively). This allocation is, to some extent, in contrast with the relatively harsh penalties (if there is such uncertainty as to who should hold responsibility, it seems strange there should be a preference for harsh regulation) the public seems to wish on organisations that breach standards. Indeed, in the same Eurobarometer survey, 51% of respondents suggested organisations which misused data should be fined, with 40% believing such organisations should be banned from using such data in the future.43

2.3.4.3 Impacts and fears

In terms of tangible impact, as a consequence of a release of information and the dangers it entailed, the public seemed specifically concerned about ID fraud, which was perceived to be a serious threat.44 This concern was relevant to both state and commercial organisations. It is curious, however, that the number of people who reported actually falling victim to this is tiny in comparison to the apparent concern. There was also undefined concern about other forms of physical or material harm. Particularly in the case of ID fraud, this may have something to do with the amount and tone of coverage the media has given the issue. Murphy points out that concern may be exacerbated by the perception that “it is very easy for people to de-fraud you and that there is very little you can do to stop it, even if you take precautions.”45 The public also demonstrated concern relating to the commercial collection and use of data. Unsurprisingly, the public approached the issue from an individual impact perspective and were concerned and annoyed by the perceived end results of data distribution, namely, direct mail, spam, cold calling, etc. The public also showed concern relating to certain data practices linked to this fear (but which also have wider significance), namely that information would be “used without knowledge”, “shared with third parties without agreement” and “that information would be used in different contexts than those in which it was disclosed”.46

---

Although there were more abstract fears relating to the combination of data and/or databases and further issues related to assemblages of data, in terms of their social basis, these were at best only loosely defined. Murphy states, "some were able to imagine an extreme scenario where these bodies ‘join up’ the information they hold, thus, to our respondents’ eyes, reducing them to pieces of (impartial) data and robbing them of their individuality". However, when listing concerns, a small portion of respondents in Eurobarometer 359 were able to recognise the more solid, individually based manifestation of these concerns; 12, 11 and 7% respectively recognised the risk of “reputation damage”, “views and behaviours being misunderstood” and “the possibility for discrimination in other areas”.

2.3.5 Justifications and benefits

Despite the fact that 63% state that disclosing personal information is a big issue for them, individuals seem to accept the need to divulge increasing amounts of information. The overarching reason for this acceptance is the rather deterministic view that it is “simply part of modern life”. On the one hand, there is the perceived obligation to release more information, both legally, as required by authorities’ increased collection practices, and practically as a price for involvement in the information environment. On the other hand, the public recognise benefits from the further release of information. Short-term benefits take the form of exchanges for rewards (or service usage). In the longer term benefits accrue from participation in data exchanges and a presence in data environments (social networking for example). However, the deterministic approach to obligatory information disclosure can arguably also be seen as a practical coping mechanism for significant power imbalances in the collection process. The processes are operating at a scale over which the individual feels very little control. Equally, formulating a position in response to increased collection may be difficult as goals and institutions may superficially remain the same, whilst the key mechanisms which drive collection and use process are imperceptible. It seems trends and effects are detached in perception from the decisions and mechanisms driving them creating the impression of inevitability.

2.3.5.1 Uncertainty and inconsistency

Whilst figures can be put on certain aspects of opinion in individual surveys, there is considerable difference between actual behaviour and opinion with respect to the stated

---

49 Ibid.
importance of privacy in online environments and behaviour in relation to privacy protection (reading privacy statements, for example).

This suggests that the model for understanding what happens with data once it is released by the individual, or what this means on an aggregate scale, is rather fluid and uncertain.

In considering the difficulty the public has in perceiving the data environment, it is of assistance to break it into two parts: Supporting technological infrastructure (and its innate capabilities) and the operation of the network of data connections and flows that constitute its lifeblood. In each consideration of technology, the public showed a significant lack of awareness as to the capabilities, uses and key privacy impacting features present (see also Chapter 2 above “Citizens’ concerns and apprehensions regarding new technologies and their applications”). This is demonstrated well in the US survey, “Technology, Security and Individual Privacy: New Tools, Threats and New Public Perceptions”51. A lack of understanding as to the shape and operation of the data flows themselves is demonstrated in “Privacy 2.0: Personal and Consumer Protection in the New Media Reality”52, in which it is pointed out that, even within the confines of a single social network, users are neither aware of the intelligent tracking technologies in operation, the connections to different applications or the dynamism of the networks in which they are taking part. From this gap in understanding, it is possible to assume that there are a series of other questions of relevance which, although they are aware of their significance, the public may not yet know what the value of their data might be, who might want this data or what the exact social or personal consequences of each release might be.53

Acquisti and Grossklags consider the possibility that “Privacy in theory may mean many different things in practice” and consequently that “the parameters affecting the decision process of the individual are perceived differently at the forecasting (survey) and operative (behaviour) phases”. They isolate a series of potential limiting factors to the individual decision to balance a transaction with a potential information security impact. The decision-making model may be unbalanced by limited information, bounded rationality issues, self-control problems and other behavioural distortions. The lack of understanding of the data environment mentioned above would certainly account for impacts on each of these potential limiting factors and thus significantly reduces the ability of the individual to “rationally” balance each action.54 Consequently, awareness of issues (and the importance of privacy and data protection) and what can be done on an abstract scale may not translate to the corresponding action in concrete situations.

Thus, whilst not unaware of dangers and the existence of structures through which data processing and protection operate, the public shows a lack of understanding as to how and why these structures operate. This provides little basis for practical decision-making in an environment in which increasing data collection and dissemination is perceived as a necessity for participation in everyday acts as well as society in general.

The broader consequences of this are, first, that the public are unable to formulate considered responses, even to identified issues as they don’t have all the information they need to do this and, second, that the public may be vaguely aware of, but largely unable to consider responses to, a series of other threats.

With respect to this second point, a number of sub-issues arise. First, the tangible impacts which are not obviously related to original data collection are ignored. Second, as the data processing itself is invisible and the processes largely not understood, the increasingly broad impact data processing has on other systems (social, economic, etc.) is correspondingly invisible. Finally, a lack of understanding of the processes means the processes themselves develop without a public presence to consider and monitor their implications and direction. The split between the necessity to operate within, but the lack of understanding of, the structures of the information society are increasingly making the public feel powerless and confused.

2.3.6 Effectiveness of regulation in light of environment

The above makes clear that the public suffers from a certain knowledge shortfall in understanding the framework and the environment it is designed to regulate. The aggregated uncertainty this creates can make it difficult to isolate specific expectations as to how and to what extent protection is expected. As a consequence, there is very little survey information on what or how the public feels is wrong with the framework or how it could be improved. This may, in itself, be indicative of a larger issue, as the public should be better able to comprehend their legal protection.

Within this uncertainty, however, the elements of protection offered are well known and the relevance of each aspect is understood and generally agreed to be important. Considering these aspects to reflect deeper principles, we find that the public do generally support the framework and its principles. A reflection of this is shown in organisations’ perceptions of the effect of the DPA on consumer trust, with 85% believing it had a positive effect.55

Yet, from the available information, the public feels that personal data does not receive the protection it should, demonstrated most obviously by the fact that a large majority feel they have lost control over their data (as well as by other opinions on protection). For example, in Flash Eurobarometer 225, a majority of respondents believed that national legislation could not cope with the demands currently placed on it.56 Whilst the

public seems not to disapprove of data protection principles, it does not perceive protection in reality to be of the same quality.

We find that it is in the enforcement and application of regulation in the data environment in which problems are perceived to lie. That the public see a problem in enforcement is demonstrated by the desire for relatively harsh measures for organisations which breach norms, whilst the uncertainty of application against the complicated current environment is demonstrated in the discrepancy and uncertainty in defining terms for even relatively basic concepts, such as responsibility allocation.

2.4 CONCLUSION

Theoretically, the public place a high value on data protection and by proxy appear to perceive the potential significance of data processing and the data environment on themselves and the societies in which they live. However, despite this awareness and even awareness of key aspects of the right, the public display a relatively superficial understanding (or at least a poorly enunciated understanding) of the broader social and legal significance of data protection.

This lack of enunciation and clarity as to the “why” of the significance of data protection parallels practical uncertainty related to the data processing environment. Whilst the public perceive certain actors as playing a key role in this environment and understand the general purposes for which these actors are using data collected, this remains an equally superficial comprehension – notably in the lack of clarification as to which connections exist between processing entities or sectors, how these connections might be of significance or how the collection of data alters the fulfilment and nature of the goals its collection seeks to achieve.

It seems that the complexity and invisibility of the processing environment leads to the lack of ability to solidly perceive trends and structures within that environment. It is apparent that the public neither comprehends, nor is often aware of the specifics or potential of the technology or software in operation or the networks and data flows operating through them. In essence, whilst there is awareness of the occurrence of further processing, what this actually entails after the first instance of collection, is perceived far from clearly. Whilst the public feel forced to act in a data environment, they feel a certain powerlessness within this environment and consider that a significant part of the decision-making and conceptualisation puzzle is missing. Thus, whilst the public is abstractly aware of issues and dangers (even at the social level), in practical terms, this does not translate into behaviour.

Accordingly, whilst the public seem to generally support the principles of the framework, there is a feeling that personal data does not receive the protection it should and that they have lost control over their data. The public perceive a problem in the enforcement of data protection rules and a discrepancy between the theory behind the framework and its applicability to the reality of the data environment.
2.5 OUTLOOK

Whilst (possibly due to the complexity of the environment making an appreciation of how the framework should apply very difficult) the question as to how to remedy the situation has been only briefly considered in surveys, there are certain instructive opinion trends which unsurprisingly all move toward clarification of the environment and the operation of the framework in relation to it. First, there is a desire for greater education about the principles and processes of the framework and environment. Second, there is a desire to solidify the fluidity of the environment (or at least elements of it); for example, 64% of Europeans believe data would be better protected by organisations if they were obliged to have a specific contact person responsible for the correct handling of data, whilst Austrians often spontaneously (outside the survey questions) suggest the need for a “one stop national authority” to be set up which could, when asked, research and provide information about the dispersion of citizen information.57

Citizens access to information: The data subject's rights of access and information: a data controllers' perspective

Raphaël Gellert, Serge Gutwirth (VUB-LSTS)

3.1 METHODOLOGICAL REMARKS

This chapter deals with the data subjects’ right to be informed (article 10 and article 11), and the right of access to data as enshrined in article 12 of the Data Protection Directive.58

We proceed in the following manner. First, we will examine the websites of some of the most important data controllers, and will assess the extent to which the information disclosed in the privacy notices is in line with the requirements of the Data Protection Directive articles 10 and 11. In particular, we will assess them against the test constituted by Opinion 2/2001 of the Article 29 Working Party (Art. 29 WP) on certain minimum requirements for collecting personal data online in the European Union,59 and Opinion 10/2004 on More Harmonised Information Provisions.60 In addition, the recent letter the CNIL addressed Google regarding the conformity of its new online privacy notice with regards to the aforementioned Opinions will be of crucial importance.

Second, we will aim at determining how data subjects can concretely exercise their right of access (if at all) from the perspective of data controllers. To this end, we contacted data controllers and asked them a list of questions concerning the data subject’s right to access, such as how many requests they have actually received or if there are differences between Member States in regard to as how the right of access to information is exercised by the European citizens.

We made a selection of five important data controllers. We chose Google, Facebook, Microsoft, Amazon and Wikimedia. Several elements have guided our choice. We based our choice upon a set of criteria that we deemed as relevant.

First, we wanted data controllers that operate in several EU states (important to see the differences in which the right of access to data can be exercised). In addition to their importance in terms of size and operational locations, we also strove to choose data controllers providing different services, commercial (e.g., Google, Microsoft, Amazon), non-commercial (Wikimedia), about communication (Facebook, Wikimedia), search

engines (Google, Microsoft), centred around one, or one type of service (Facebook, Wikimedia, Amazon), or on the contrary, providing a multiplicity of services (Google, Microsoft).

We will therefore inspect the privacy notices of the following data controllers: (1) Facebook; (2) Google; (3) Microsoft; (4) Wikimedia; (5) Amazon.

3.2 **THE DATA SUBJECT’S RIGHT TO INFORMATION AND OF ACCESS TO DATA**

Article 10 of the Data Protection Directive states:

> "Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
> (a) the identity of the controller and of his representative, if any;
> (b) the purposes of the processing for which the data are intended;
> (c) any further information such as
> - the recipients or categories of recipients of the data,
> - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
> - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."

Just as any provision of the Data Protection Directive, this provision is subject to implementation in the national legislation of each Member State. However, the Article 29 WP has striven to clarify and harmonise this obligation in its Recommendation 2/2001 on certain minimum requirements for collecting personal data online in the European Union, and in its Opinion 10/2004 on More Harmonised Information Provisions.

In its Recommendation 2/2001, the Art. 29 WP makes explicit which information should be contained in privacy notices. In order to be lawful, a privacy notice should therefore contain the following information. It should state the *identity* and physical and electronic address of the controller; clearly state the *purpose* of the processing for which the controller is collecting data; to state clearly the *obligatory or optional nature* of the

---

61 The right of the data subject to be informed is contained within two articles, namely article 10 and article 11. Article 10 foresees the situation where the data have been collected from the data subject himself, whereas article 11 deals with personal information that has not been retrieved from a third party. In this chapter, we only discuss the situation where the data have been collected from the data subject.


information to be provided (information is obligatory when it is necessary to carry out the service requested); to mention the existence of and conditions for exercising the rights to consent or to object to the processing of personal data, as well as to access and to rectify and delete data (in this case, information should be provided, first, concerning the person or service to be addressed to exercise these rights, and, second, regarding the possibility of exercising them both online and at the physical address of the controller); to list the recipient or categories of recipient of the collected information; to indicate whether non-EU countries where the information might be transferred provide adequate protection in the meaning of Article 25; to indicate the name and address (physical and electronic) of the service or person responsible for answering questions concerning the protection of personal data; to mention clearly the existence of automatic data collection procedures before using such a method to collect any data; to point out the security measures featured by the website. Furthermore, the information should be provided in all the languages used on the site, and the data controller should check the consistency of these information should they be disclosed in various sections of the website.64

Whereas Recommendation 2/2001 of the Art. 29 WP makes explicit which information should be contained in the privacy notices of data controllers, Opinion 10/2004 spells out some principles that should guide the elaboration of privacy notices. Some of these principles are of interest to us. According to the Working Party, good quality privacy notices tend to improve the quality of citizens’ data protection. This entails the need to present information with meaningful and appropriate content to the data collection situation, especially with a view of providing the data subject, in simple unambiguous and direct language, with the information that is most important for him or her to know, and the information that he or she most likely wants to know.65 Privacy notices respecting these principles should lead to an improved awareness on data protection rights as well as to an enhanced quality of information on data protection.66 Therefore, in addition to the linguistic issue and the need for clarity and understanding of the data subject, there is a strong emphasise put upon the quality of the information provided.

Accordingly, the Art. 29 WP distinguishes between two types of information. There are essential information, namely, the identity of the data controller and the purpose of the data processing, and there is the “possible further information”, which includes the recipient of the data, the response obligation, and the existence of access and rectification rights. This division (between essential and further information) paves the way for the multi-layered approach of the Art. 29 WP. According to the latter, a sound privacy notice can be divided into three layers. First, the short notice contains the so-called essential information.67 Second, the condensed notice contains “all relevant information required under the Directive”, i.e., “possible further information”.68 Third,

66 Ibid., p. 6.
67 Ibid., p. 8.
68 Ibid., p.8.
the full notice must, in addition, include all national legal requirements and specificities.69

The aim of this three-layered structure is to achieve the core objective of notices, that is, the need for easily understandable, in other words, effective knowledge. Therefore, one should not engage in an overly literal reading of the framework. In our opinion, the matter of crucial importance is to provide privacy policies that provide different levels of accuracy. Hence, differentiating between “essential information” and “possible further information” is one means to reach this aim, but certainly not the only one. Data controllers who provide multi-layered privacy notices, though not strictly respecting the structure recommended by the Art. 29 WP, should nonetheless be given credit.

In reaching the aim of effective knowledge, the multi-layered framework puts the emphasis upon formal requirements. However, formal criteria are not sufficient alone. There must also exist substantial criteria to assess whether these privacy notices are empty words, however well hierarchized they may be. Of course, a multi-layered framework might help in this as providing increased details should, in theory, lead to a more thorough knowledge. Yet, it provides little guidance as how to assess privacy policies from a substantial viewpoint. In this respect, we might find information in a letter the Commission nationale de l’informatique et des libertés (CNIL), the French Data Protection Authority (DPA), recently addressed to Google concerning its new privacy policy.70 As will be seen later on (cf. individual assessment of the different privacy policies), it critically assesses which information can be concretely obtained from this privacy policy.

As a conclusion, we find that privacy policies must obey several criteria. A first requirement relates to the type of information that must be contained therein. A second requirement concerns the quality of such information, which must be effective. This entails obligations both from a formal point of view (three-layered approach) and from a substantial viewpoint (CNIL letter to Google).

With these considerations in mind, we have assessed the privacy notices of aforementioned data controllers.

In inspecting their privacy notices, we put the emphasis of our analysis on a few elements that we consider to be the most pertinent. Namely, we assess the extent to which they make known what information they store, for what purpose, for how long and whether those data are shared with others (and, if so, who), and how easy or difficult it is for citizens to view the personal data held on them and how easy or difficult it is for them to correct such data.

69 Ibid., p. 9.
70 The letter is available at the following address: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120227_letter_cnil_google_privacy_policy_en.pdf
3.2.1 Google

What kind of data does Google collect?

Google\(^{71}\) distinguishes between two types of information: classical personal information mobilised by the user to create a user profile, which is qualified as “information you give us”; and “information we get from your use of our services”, that is, the personal information disclosed by a user when making use of Google’s services, and which includes device information, log information (e.g., search queries, IP address, browser information, etc.); location information in the case of location-enabled services; unique application numbers; cookies and anonymous identifiers, etc.

Purpose

Google states that the main purpose justifying its collection of users’ data is “to provide better services to all of our users”, including “tailored content – such as giving you more relevant search results and ads.” Beyond this very general purpose, Google engages in making more explicit what providing a better service means. This may include Google using “information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we’ll be able to provide you our services in your preferred language”; or combining “personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know.”

We share the opinion of the CNIL, contained in the letter it recently addressed to Google concerning its new privacy policy. In this letter, the CNIL argues that “the new privacy policy only provides general information about all the services and types of personal data Google processes. As a consequence, it is impossible for average users who read the new policy to distinguish which purposes are currently relevant for their use of a particular Google service.” It therefore goes on to request that Google “supplements existing information with purpose specific information”.\(^{72}\)

For how long does Google store the data?

There is no information available as to the duration for which the collected data are stored.

Access, rectification (including responsible person for handling complaints)

There seems to be confusion as to the meaning of access. In Google’s interpretation, access is only about the first category of personal information, that is, the classical identifiers that the user has voluntarily disclosed in order to create a profile. Thus, the whole purpose of Google’s access procedure would be to enable the user to correct any wrong personal information he disclosed to Google. However, the right of access is about

---


much more than that: it is about determining which data are *concretely being processed*. This includes equally what Google qualifies as “information we get from your use of our services”. For instance, this is a description of the result of Austrian student Max Schrem exercising his right of access towards Facebook: he “received a CD filled with pictures, posts and much other profile data, including for example dates, tagged people and geo-locations of uploaded images, friend requests, pokes, etc. However, much information was still missing from the data set, such as likes, comments on other people’s walls, data about face recognition, FriendFinder, advertising activities, the use of Facebook plug-ins on external websites, and more.”  

This clearly shows that accessing the personal information one voluntarily disclosed is quite far from what the actual right of access should be. Additionally, there is no indication as to who can be contacted in order to exercise this right, or how this should be done.

*List of recipients*

Google provides a list of third parties to whom it may disclose users’ personal information. It does so in the following situations: “With your consent”, with domain administrators, for external processing, i.e., with business partners to whom Google sub-contracts some of the processing of data entailed by its services; for legal reasons. Furthermore, it may also share “aggregated, non-personally identifiable information publicly and with our partners, such as publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.” Also, if “Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.”

*Assessment of the privacy notice*

All in all, Google’s privacy policy seems unsatisfactory. Our main criticism is that it is overly broad and general.

As the CNIL suggests, one way of justifying this criticism is to remember that Google, under pretexts of transparency and simplification, has elaborated a single privacy policy for all its services. As the CNIL puts it, “Google’s online services are numerous and differ greatly both with regard to purposes and types of data they process. The new privacy policy provides only general information about all the services and types of personal data Google processes. As a consequence, it is impossible for average users who read the new policy to distinguish which purposes, collected data, recipients, or access rights are currently relevant for their use of a particular Google service.” As outlined in the

---

75 Google will share users’ data for the following reasons: to “meet any applicable law, regulation, legal process or enforceable governmental request; enforce applicable Terms of Service, including investigation of potential violations; detect, prevent or otherwise address fraud, security or technical issues; protect against harm to the rights, property or safety of Google, our users or the public, as required or permitted by law.”, available at https://www.google.be/intl/en-GB/policies/privacy.
“purpose” section, Google intends to combine users’ data across its services. According to the CNIL, this makes it very difficult if not impossible (even for privacy professionals, let alone average users) to determine which data are being combined between which services. As a matter of fact, Google’s tutorial video states very clearly and explicitly that the aim of unifying its privacy policies is to provide users’ with personalised services, thereby triggering concerns as to the existence of opaque automated processing of personal data.76

The shortcomings are also important as far as information regarding the right of access to data is concerned, not only because of an elusive definition of access that doesn’t match that of the Data Protection Directive, but also because there are no indications whatsoever as to who can be contacted, or which form can be used to do so. It is not an overstatement to argue that the current state of information is not satisfactory enough in order to enable users to duly exercise their right to access.

On the other hand, one has to acknowledge the existence of so-called privacy tools. These tools are meant to endow the data subject with a greater control over his or her personal information in the framework of the use of Google’s services.77 For instance, the Google Dashboard informs the user about information related to his account, e.g., what he posted on this service, or who has access to his mail, etc. “Account Activity” provides information on how much one has used the different services, from which computers and browsers, etc. “Ad preferences” is a tool to personalise advertisements displayed by Google. These tools represent a positive measure insofar as they give the user some control over the information he or she decides to disclose to Google. Because they enable the user to manage what information can actually be processed by Google, they have a strong kinship with the right of access to information. Yet, as such, they do not account for a valid implementation of the right of access, as they do not disclose all the information processed by Google.78 They cannot simply replace the right of access (which entails specific procedures to contact the data controller), but rather they should act as a complement. Additionally, these transparency tools seem to contradict Google’s very own notion of personal data as solely containing classical biographical identifiers as they include all data relating to the user.

As a matter of fact, the main criticism that could be made to Google’s privacy notice is that of over-simplification. Indeed, it looks like it tried to make one simple notice for all its services. While such an effort of simplification deserves to be acknowledged (assuming it is undertaken in good faith), this shouldn’t however lead to incomplete information that would be incompatible with the requirements of articles 10 and 11 of the Data Protection Directive as they have been interpreted and outlined by the Art. 29 WP. In this respect, it would have been appreciated had Google taken steps to implement the multi-layered approach advocated by the Art. 29 WP in its Opinion 10/2004 on More Harmonised Information Provision. This is a good example of why the framework provided by the Art. 29 WP should not be interpreted in an overly literal manner. We are indeed of the opinion that instead of relying upon the “essential/non-essential

76 Video scan be found at this address: https://www.google.be/intl/en-GB/policies/privacy/videos/
information” dichotomy, the different layers could have been organised around the different types of services that Google offers.\footnote{For example, one could imagine a first layer where similar services are grouped together, a second one where each service is individually described, etc.}

### 3.2.2 Microsoft

**What kind of data does Microsoft collect?**

Microsoft\footnote{Address of the privacy policy: \texttt{http://privacy.microsoft.com/en-us/default.mspx}. Any further quotes in the section dedicated to Microsoft without explicit reference refer to Microsoft’s privacy policy.} collects different types of personal information. In addition to collecting traditional identifiers (e.g., names, addresses, etc.) that are necessary in order to create an account, Microsoft also collects additional information about users’ interactions with Microsoft sites and services such as IP address, browser type and language, access times and referring website addresses. Microsoft also undertakes automated processing of users’ data through website analytics tools, “to retrieve information from your browser, including the site you came from, the search engine(s) and the keywords you used to find our site, the pages you view within our site, your browser add-ons, and your browser’s width and height,” but also on third-party websites. Cookies and Web beacons are also used in order to determine what actions have been undertaken on the website.

**Purpose**

“Microsoft collects and uses personal information to operate and improve its sites and services.” Improvement of Microsoft’s websites and services must be understood in the meaning of ever-greater personalisation and customisation. It is precisely for this purpose that “information collected through one Microsoft service may be combined with information obtained through other Microsoft services” and that Microsoft “may also supplement the information it collects with information obtained from other companies”.

In addition to this general “service improvement purpose”, Microsoft also outlines another purpose: direct communication with its users, e.g., mandatory service communication, but also, subject to opt-out, promotional mailings.

**For how long does Microsoft store the data?**

No details are provided.

**Access, rectification (including Responsible person for handling complaints)**

As is the case for Google, Microsoft interprets the data subject’s right of access to data merely as the possibility to view and edit the personal information disclosed in order to create a user profile. However, as we have seen it before, this is far from corresponding to what the right of access to data is really about: being informed of the data that are being concretely processed by the data controller. However, unlike Google’s policy, Microsoft provides a general web form in case a user should complain, but does not
specifically indicate that it is to be used for purposes of the right to access, nor does it provide for a physical address in such case.

**List of recipients**

Microsoft provides a list of situations wherein they might disclose users’ personal information to third parties. It might do so in case the user has consented, and in case a service is jointly operated with a third-party firm or is a subcontracted a service. It might also disclose users’ personal data in the following cases: in order to “comply with the law or respond to lawful requests or legal process; in order to protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or in order to act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public. We may also disclose personal information as part of a corporate transaction such as a merger or sale of assets.”

**Assessment of the privacy notice**

There are some important inaccuracies. First, Microsoft relies upon a very narrow definition of personal data that would solely include classical biographical identifiers. According to Microsoft, this would mean that data relating to users such as IP addresses are not considered as personal data. This is a very narrow view, with which many have disagreed. For instance, the Art. 29 WP – basing itself upon the open-ended definition of personal data in the Data Protection Directive – has come with a very broad, though not uncontested, opinion on the concept of personal data.

According to the Directive, personal data is any data that relates to an identified or identifiable individual.

The Art. 29 WP considers that data can relate to an individual under three non-cumulative criteria: content, purpose or result. Either the content of the data is about a person, either the information is not about a person but is used with the purpose of taking actions on this person, or the information, although not about the person, can be used with an impact on this person. As a matter of fact, the extent of what can be an identifier has to be examined on a case-by-case basis.

In addition to this, the person needs to be identified or identifiable, that is, even though the person is not identified yet, it is possible to do so. In order to determine whether a person is identifiable or not, Recital 26 of the Directive provides that “whereas to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller, or by any other person to identify

---

81 This definition of personal data echoes that of Google's privacy policy.
82 According to article 2(a) of the Directive, “'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
84 Ibid., p. 12.
85 Ibid.
the said person”.86 The criterion of all of the means reasonable should take into account all of the means that are concrete and not include a mere hypothetical possibility.87 

Given these premises, it is evident for the Art. 29 WP that IP addresses should count as personal data.88 This proposition had actually already been made some 12 years ago in its Working Document entitled "Privacy on the Internet – An integrated EU Approach to Online Data Protection”.89 By the same token, it can be argued quite confidently that the other data released by the user and/or concerning its device can count as personal data.

Furthermore, Székely et al. have coined the notion of the “individual fingerprint”, whereby the use of several non-strictly personal data concerning one particular individual will lead to an “individual fingerprint”, which as such must be regulated as personal data.90

Like Google, Microsoft has only one privacy policy for its whole range of services. Hence, the same criticism applies, i.e., the information provided is far too broad for an average user to determine which purposes, collected data, recipients or access rights are currently relevant for its use of a particular Microsoft service. But beyond the issue of a single privacy policy applying to all of Microsoft’s different services, we remain convinced that the level of generality is too high. A purpose such as “improving the quality of a service” is very broad and elusive, and can justify far too many processing operations in our opinion. Better use of the three layers framework advocated by the Art. 29 WP in its Opinion 10/2004 on More Harmonised Information Provisions could have been proven very useful.

Furthermore, there is insufficient information concerning the fact that Microsoft undertakes automated processing of personal data.

---

86 We put the emphasis.
87 The Art. 29 WP takes a pragmatic approach by stressing that this criterion should take all the factors at stake into account. This includes the cost of conducting the identification, the intended purpose, the way the processing is structured, the expected advantages, the interests at stake for the individual, the risks of organisational dysfunctions (e.g., breaches of confidentiality duty), and technical failures. Furthermore, the test should take into account the real-time level of technological development. Special importance must be given to the purpose of the data controller. Article 29 Data Protection Working Party, “Opinion 4/2007 on the concept of personal data”, Working Paper 01248/07/EN, WP 136, Brussels, 2007., p. 12.
88 Ibid., p. 16.
3.2.3 Facebook

What kind of data does Facebook collect?

Facebook processes several types of personal information. Regarding the information the user voluntarily discloses, Facebook receives registration information (e.g., name, e-mail address, birthday, gender, etc.), but also the information users want to share when using Facebook services (e.g., posts, status update, add a friend, like a page, etc.). Facebook also collects a user’s information not disclosed by the user herself. It collects information shared by other users of the service, which includes tagged photos or being added to a group. Facebook collects information from the user’s use of the website. This includes data relating to the use of Facebook (e.g., visit of profiles, friend search, etc.), as well as metadata related to these activities (e.g., time, place, date, etc.). In addition, Facebook collects information from the devices used to log the website, which includes IP address, URL, information about the browser, visited pages, the operating system of the device, etc. It might also collect information from advertising partners, or any partner (such as how a person responded to an ad).

Purpose

Facebook uses the information at its disposal “in connection with the services and features it provides to its users”, with the ultimate goal of improving its services. Following this logic, Facebook might use this information for the following purposes: to keep Facebook secure; provide users with new, improved services (e.g., location services); measure the effectiveness of ads; make suggestions to users (e.g., new friends).

For how long does Facebook store the data?

Facebook stores the data as long as the user is enjoying the service. In case the user wants to stop using her account, there are two possibilities, either deactivating the account or deleting it. Only in this second case will the account be properly deleted. It takes about 30 days to fully delete an account.92

Access, rectification

Facebook’s implementation of the right to access has evolved through time.

Previously, it used to provide a specific online form so that users could exercise this right to access. However, since 4 November 2011, Facebook removed it after it received thousands of requests. An online tool has replaced it. However, the website “Europe versus Facebook” discourages users from having recourse to it as it only provides an incomplete list of data. As it is, “when using this tool you only get a copy of your profile, but non of the data Facebook holds or generates in the background. This means you only

91 http://en-gb.facebook.com/about/privacy/. Any further quotes in the section dedicated to Facebook without explicit reference refer to Facebook’s privacy policy.
92 Yet, it appears that Facebook keeps archive of supposedly deleted content. See for instance, http://www.guardian.co.uk/technology/2011/oct/20/facebook-fine-holding-data-deleted?cat=technology&type=article
get about 29% of your data! Further, it would seem that using this online tool entails losing the possibility of exercising the full right of access.

The only possibility to exert this right is by sending a request to Facebook, either through e-mail or via regular mail. However, although a procedure to send e-mails exists, Facebook does not specify whether this procedure can be used for purposes of access to personal data, nor does it mention the person responsible for handling complaints or of the physical address to which requests must be sent.

Facebook explicitly states that it will provide an initial response to access requests within a reasonable period of time, which is typically 40 days, although it seems that this deadline is never respected in practice.

*With whom does Facebook share our personal data?*

Facebook shares users’ personal data in case of user consent or in the cases provided for in its policy, which include responding to legal requests or preventing harm such as fraud or other illegal activity, joint service providers or subcontractors. In case of change in the ownership of Facebook, the data will be transferred to the new owner.

*Assessment of the privacy policy*

It seems to us that the Facebook privacy policy present some positive aspects.

First, unlike Microsoft or Google, Facebook provides only one type of service. Therefore, its privacy policy matches the type of service provided.

Second, it seems to make a good use of the multi-layered framework of the Art. 29 WP, as the first page of the policy is a quite general one, outlining the different categories of issues it tackles (e.g., use of information, sharing of information, advertisement. It also features a link to the full policy, and a link to so-called “interactive tools”. Like Google’s privacy tools, these interactive tools are meant to help the user to better manage her information. However, unlike Google, where the tools give concrete and valuable information on which personal data are processed by Google, Facebook’s tools mainly focus on the privacy parameters of Facebook insofar as it is a social network with the exception of the tool to download information.

Unlike other policies, Facebook mentions both the duration for which personal data are being stored, and the procedure to have them removed.

---


94 Ibid.

95 Ibid.

96 In addition to these, one needs remember that, as stated in the section on the type of data processed, Facebook processes data from advertising partners, which entails exchanging data with the latter. See, [http://www.pcworld.com/article/254636/which_facebook_apps_steal_your_data_and_how_to_stop_them.html](http://www.pcworld.com/article/254636/which_facebook_apps_steal_your_data_and_how_to_stop_them.html).

97 Although one could argue that it provides several services, one also has to acknowledge that it all revolves around the core service of social networking, contrary to Microsoft or Google, which provide a plurality of heterogeneous services.

However, there are also shortcomings. As was the case with other data controllers, one shortcoming concerns the substantial requirements of privacy policies. The purpose is defined in an overly broad manner that makes it impossible to exactly understand to what type of operations users’ data are subject. This is especially true of automated operations undertaken by Facebook. From a substantive perspective, it would seem that Facebook has developed a correct understanding of the notion of personal data as it encompasses information related to the device of the user. Yet, this might be of little practical help as we have described the ambiguities revolving around the possibility of exercising the right of access.\(^9\)

### 3.2.4 Wikimedia

The Wikimedia\(^{10}\) privacy policy applies to all the projects featured by the Wikimedia Foundation, namely, Wikipedia, Wiktionary, Wikiquote, etc.\(^{10}\)

**What kind of data does Wikimedia collect?**

As a collaborative website, the content of Wikimedia is dependent upon the contribution of its users. These contributions are not covered by Wikimedia’s privacy policy, which applies solely to the data collected by Wikimedia.

Wikimedia stores device information such as IP addresses and raw logs of transactions on its website. It says it does not process more information regarding non-logged users who simply intend to visit pages.

When users log in and/or intend to contribute to Wikimedia, other types of processing take place. Edits are identified with the username or network IP address of the editor, and editing history is aggregated by author in a contribution list. There is a difference between logged in users, whose IP address will be collected only in cases of abuse (e.g., vandalism on a Wiki page). Cookies are also used, both for readers and editors. Users’ contributions are aggregated and made publicly available and include data relating to time and the number of edits.

**Purpose**

The overall purpose justifying the processing of data by the Wikimedia Foundation is the “well-being of its projects”. Such a general purpose includes, but is not limited to, the following goals: to enhance the accountability of the project (in cases of abusive activities, it is important that the responsible users be identified); to provide statistics; to help solve technical problems.

---

\(^9\) Among many stories of users unsuccessfully trying to retrieve their data from Facebook, the most famous one is undoubtedly about Max Schrem, see, [http://www.sueddeutsche.de/digital/datenschutz-aktivist-schrens-der-mann-der-facebook-nervt-1.1337259](http://www.sueddeutsche.de/digital/datenschutz-aktivist-schrens-der-mann-der-facebook-nervt-1.1337259).

\(^{10}\) [http://wikimediafoundation.org/wiki/Privacy_policy](http://wikimediafoundation.org/wiki/Privacy_policy). Any further quotes in the section dedicated to Wikimedia without explicit reference refer to Wikimedia’s privacy policy.

For how long does Wikimedia store users’ personal data?

Editing history, which includes the user name and/or the IP address of the editor, is available permanently on the projects. In case they are collected, IP addresses of logged-in users will be stored only for a limited time, although this period is not made explicit.

Access, rectification

Quite surprisingly, there is no mention to the right of access to data in the meaning of the Directive. The Wikimedia privacy policy uses access to data as a way to determine which individuals have access to user’s personal information (e.g., elected community users, or specific Wikimedia employees). Moreover, as such, the privacy policy does not include the details (neither electronic nor physical) of the responsible person for handling privacy related complaints, and one must thus assume that the general “Contact us” section is to be used for this purpose as well.

List of third parties with whom Wikimedia may share users’ personal data

Wikimedia may disclose the user information at its disposal in the following situations: in response to a valid subpoena or other compulsory request from law enforcement; with permission of the affected user; when necessary for investigation of abuse complaints; where the information pertains to page views generated by a spider or bot and its dissemination is necessary to illustrate or resolve technical issues; where the user has been vandalizing articles or persistently behaving in a disruptive way, data may be released to a service provider, carrier, or other third-party entity to assist in the targeting of IP blocks, or to assist in the formulation of a complaint to relevant Internet service providers; and where it is reasonably necessary to protect the rights, property or safety of the Wikimedia Foundation, its users or the public. In the event of a court order, Wikimedia will attempt to notify the affected user within three days.

Assessment of the privacy notice

Although Wikimedia features only one privacy policy for several services, this does not impact its quality to the same extent as for Microsoft or Google for one simple reason, all of the services provided by Wikimedia are of the same nature: they are collaborative projects relying upon the contributions of users, whereas Microsoft and Google provide for heterogeneous services that are different both in nature and scope.

For the rest, it is quite specific as to the ways personal are being processed, and as to which personal information is processed. Its major weakness lies in the complete absence of information as to the right of access.

A positive element is the purpose, the definition of which is much more precise and accurate than the privacy policies of the other four organisations examined in this chapter.

Another element of criticism lies in the balance that Wikimedia tries to strike between the need to be comprehensive and the need to be simple, clear, accessible and transparent. Its privacy policy is indeed clear and structured, but it could have made use
of the three-layered structure framework, since Wikimedia's policy consists of a single layer. Furthermore, no information is given concerning the conditions for exercising the right of access to data.

Interestingly, Wikimedia makes explicit mention of the principle of data minimisation. Also, the fact that it pursues non-commercial objectives is probably the reason why it doesn’t engage in cross-service aggregation of user data, an activity which is quite opaque in the cases of Google or Microsoft.

3.2.5 **Amazon**

*What kind of data does Amazon collect?*

Amazon collects different types of personal information. It collects information users disclose, such as when they create a profile, but also information that stems from their actions as is the case when they search for a product. It also collects what is being referred to as “automatic information” (i.e., information from the user’s device), such as the IP address, browser information, and other metadata such as length of visit to certain pages and page interaction information. This data is also aggregated with similar information from other users. Amazon might also receive information from other sources, such as page-view information from some merchants with which Amazon operates co-branded businesses.

*Purpose*

Amazon solely states that the only purpose for which its collects and further processes users’ data is to help them “personalise and continually improve the shopping experience at Amazon.com.” No other sub-purpose is specified.

*For how long does Amazon store users’ personal data?*

Amazon does not specify the duration of the collection and storage of the data.

*Access, rectification*

Amazon provides adequate information as far as the right to access is concerned, since it states that users can have access to a “broad range of information concerning them, their account, and their interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information.” However, Amazon provides no information on how to access this very information, or whom to address in the instance of complaints.

*With whom does Amazon share our data?*

Amazon seems to share its users’ information only in a very limited number of cases. It shares our personal data with other businesses who are jointly offering a service, or who

---

are sub-contractors for a service. It will also be the case should Amazon.com be sold or bought by another business; and in any situations required by law.

Assessment of the privacy notice

Amazon’s policy presents some positive elements. Overall, the information it provides is quite comprehensive, and it tackles all of the topics, including the right of access to data. Furthermore, the information is well structured, with a synthesis of all of the points addressed preceding the actual notice, for the sake of clarification. In the same vein, examples are usually accessible via a link that takes the user to the complete information available on a determine issue. This recalls the multi-layered system of information advocated by the Art. 29 WP in its Opinion 10/2004.103

However, it also presents some shortcomings. First, it is far too general about its purposes, and thus makes it quite difficult for users to concretely assess the purposes for which their data are being processed. Second, the right of access seems to be insufficiently presented. There are some inconsistencies with the information released concerning this right. On the one hand, Amazon is one of the very few websites that commits no mistake about what this right is really about and is very explicit about the possibility to exercise it with regard to users’ information in its possession. On the other hand, it provides absolutely no information as to how concretely the user can exercise this right. Contrary to Facebook (which is the other data controller correctly explaining what the right of access to data is about), Amazon provides no procedure as to how this right can be exercised. This shortcoming could have been circumvented if Amazon had provided the address (either physical or electronic) of the person responsible for the exercise of this right. Furthermore, the “contact us” section of the privacy notice is not easy to find, and it leads to an e-mail drafting software featuring a pre-existing list of topics, amongst which there is no mention of privacy-related issues, nor about the exercise of the right to access.

3.2.6 Conclusions

We attempt to draw some lessons and single out some patterns from our analysis of the privacy policies that we have examined.

As far as the information is concerned, some types of information are usually disclosed in a satisfactory (and quite similar) way. For instance, the type of information processed is well explained. All of the data controllers make the difference between the information the user voluntarily discloses and the information that is retrieved from him through his device. Some of the controllers (e.g., Google, Microsoft) are quite ambiguous as to the nature of personal data in this second category and only consider voluntarily disclosed information as personal data (this has some consequences on the way they frame the right of access in their policies). Yet, in spite of this inaccuracy, all of the data controllers provide a comprehensive list of all the data related to the users that are being processed. Other information provided in a comprehensive manner is that of the list of third parties with whom the controllers share our data: all data controllers

provide a reasonably complete list, which is often nearly identical. Data controllers are more ambiguous on the duration of their respective processing. In some cases, such as Facebook, the controller states that only the complete deletion of the profile will put a definitive end to the storage and further processing of data, or Wikimedia, which states that collected IP addresses will only be stored for a determined amount of time. The other data controllers do not provide details, and one can assume this means the data is stored indefinitely.

Another contentious point is that of the purpose of the processing. In all cases, the purpose of the processing is defined in very broad terms. Apart from Wikimedia, which details its purpose in a closed list of sub-purposes, all the other (commercial) data controllers define the purpose of their processing operations as the improvement of their services. This makes it hard to concretely determine what data processing operations the controllers carry out, especially when the data controller states that it will aggregate the personal information of its users from its different services and/or from third-party controllers with whom it jointly proposes services. Finally, the last element of information concerns the right of access to data. In this case too, the information provided by the different data controllers is scarcely satisfactory. In our understanding, there are two categories of data controllers: those who misconceive the right of access to personal data and the information that should relate to it, and those who, although they understand the right of access properly, fail to successfully inform the users about it. The first category comprises those controllers who understand access to data as access to the data voluntarily disclosed (Google, Microsoft), and of those who understand it as way to determine who has access to the users’ data (Wikimedia). The second category comprises controllers who understand the right of access correctly but fail to explain how to exercise it (Amazon), and of those who understand it correctly, provide explanations about how to exercise this right online but nonetheless fail to provide full and complete information about it (Facebook).

At this point, we have two remarks. First, we make the distinction between what could be referred to as “linear” and “reflexive” information. Linear information includes straight-forwards facts such as the type of data processed or the third parties to whom it is disclosed. Usually, this type of information is satisfactorily laid out. Reflexive information, however, refers to information requiring a minimum of explanation and construction. This is typically the case for the purpose of the processing or the right of access, and it seems to us that this is the issue the CNIL tried to address in its letter to Google. It is striking to see that most data controllers consistently fail to live up to the benchmark of the CNIL letter to Google. Second, some of the shortcomings observed might have something to do with the issue of applicable law. Because all five data controllers examined in this chapter process data through a website, issues of applicability of data protection legislation should come to the fore. We could thus make the hypothesis that some of the shortcomings observed in the privacy policies might be due to the fact that the data controllers deem themselves not to be bound by the EU Data Protection Directive. Apparently, that is Google’s view, as it claims that its EU-based subsidiaries do not process any user data, and thus are not obliged to provide for a right to access.104 Such an argument is fallacious. Under the current regime, the question of

---

104 Ball, James, “How to download your data from Google and Facebook”, *The Guardian*, 22 April 2012. 
http://www.guardian.co.uk/news/datablog/2012/apr/22/download-your-data-google-facebook?fb=native
applicable law is regulated by article 4 of the Directive. The main rule is provided by article 4(1)(a), which uses the criteria of the establishment of the data controller: the data controller will be subject to the law of the country where it is established.\(^{105}\) However, article 4(1)(c) provides that the national law might also apply in cases where the equipment used to collect data is situated in the EU, though the controller itself is not established within any Member State.\(^{106}\) The notion of equipment is further specified in Recital 20 of the directive, which mentions “any means used”, and must thus be understood in a broad way.\(^{107}\) A clear example of a means used that would trigger applicability of the Directive is that of cookies,\(^{108}\) which all the data controllers we have analysed are using. Consequently, no data controller should be in a position to claim that the provisions of the Directive on the right to information and the right of access do not apply to it. Yet, it has been acknowledged that this provision of the Directive is problematic as it might lead to conflicts of applicable legislation by overextending the reach of EU legislation.\(^{109}\) Still, this argument does not hold. Even if Directive 95/46/EC did not apply, all of the data controllers discussed are based in the US, and as such, subject to the US privacy act, which foresees both a data subject right to be informed, and a subject right of access to data.\(^{110}\) Furthermore, it could be argued that by refusing to entrust the processing of personal data to their EU subsidiaries data controllers have in mind not to be subjected to EU law. Bygrave acknowledges such a situation as being an adequate case for the prevalence of EU law over national law in accordance to article 4(1)(c).\(^{111}\) In any event, we are of the opinion that EU law applies to these data controllers as they have offices in several EU countries (some even have EU headquarters) that clearly process EU citizens’ data.\(^{112}\)

\(^{105}\) Article 4(1)(a) provides that national legislations adopted pursuant to the Directive shall apply where “the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.”

\(^{106}\) Article 4(1)(c) provides that national legislations adopted pursuant to the Directive shall apply where “the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.”

\(^{107}\) Recital 20 states that “whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.”


http://www.justice.gov/opcl/privstat.htm


\(^{112}\) It is to be noted that these complicated rules on applicable legislation will be modified in the proposal for a Regulation towards more simplicity. The criterion of “equipment” is replaced by the criterion of “data subjects residing in the EU”. The effect of these changes is to bring more non-EU-based companies offering services over the Internet within the reach of EU law. See European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection
As far as the structure of the privacy policies is concerned, the correct implementation of the Art. 29 WP’s Opinion on More Harmonised Information Provisions seems mitigated. With the single exception of Wikimedia, all of the data controllers have published their privacy policies according to some type of multi-layered framework. Although such framework does not strictly respect the criteria laid down by the Art. 29 WP, it is nonetheless quite satisfactory in some cases (Facebook, Amazon). Data controllers proposing different types of services tend to propose a single, unified privacy policy that has some affiliation with the multi-layered approach advocated by the Art. 29 WP. However, if one can only applaud this search for simplicity and ease of comprehension, this cannot be achieved at the expense of the quality of the information provided, which is often the case when there exists one single policy that applies to services that are quite different in nature (Google, Microsoft).

3.3 THE DATA SUBJECT’S RIGHT OF ACCESS TO DATA

3.3.1 Principles, caveats, and methodology

Article 12 of the Data Protection Directive states:

“Member States shall guarantee every data subject the right to obtain from the controller:
(a) without constraint at reasonable intervals and without excessive delay or expense:
- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.”

The articles makes clear that the data subject’s right of access to data is an active right. If one reads carefully, it entails two main things: confirmation as to whether or not some of his personal data are being processed, and in case of positive answer, communication of these very data.


Different from the right to be informed, which could be described as a static right, and which provides general information describing which types and categories of data are being processed, for what purpose and disclosed to whom, the right of access could on the contrary be described as a dynamic right. It is about enabling the data subject to determine concretely which of his or her personal data the data controller is being processed.

In its Communication on “A comprehensive approach on personal data protection in the European Union”, the European Union emphasised the fact that the right of access to data is a key element to provide the user with enhanced control over his or her personal data.114 This is consistent with the proposal for a Regulation, which, among many things, strives to empower the data subject, inter alia, by granting him new prerogatives.115 However, exercising this right does not prove to be an easy task for several reasons.

First, the modalities for exercising this right are determined by each Member State in its law implementing the Data Protection Directive, and it might thus differ from one State to another. For instance, according to the Information Commissioner’s Office (ICO), one can exercise the right of access to data in the UK by sending a letter or an e-mail to the data controller. Data subjects are encouraged to provide enough information to identify themselves (the ICO website mentions that “it is a good idea to include your full name and address in the heading, and any other information to help identify you”), and to keep a copy of their mail or e-mail.116 In Italy, the Italian DPA (the Garante per la protezione dei dati personali) underscores that no particular formalities are necessary in order to exercise these rights.117 The French CNIL suggests that the right of access to data can be exercised by anyone able to prove their identity.118 In Belgium, data subjects should also prove their identity, preferably by enclosing a copy of their identity card.119 Spain may have the most formalistic rules, as it requires a data subject to send a written letter containing a copy of their identity card.120 In addition to the diverging national rules prescribing how to exercise one’s right of access, there is a lack of certainty surrounding rules on applicable law, which apply criteria linked to the data controller.121 This will especially be pertinent in our case since we deal with online data controllers. Therefore, data subjects might not be in a position where they are able to determine which rules apply to their request of access to their personal data. Furthermore, in some cases, the data subjects might find that the applicable law is not that of their State of residency,

116 http://www.ico.gov.uk/for_the_public/personal_information/how_manage/access_info.aspx
117 http://www.garanteprivacy.it/garante/doc.jsp?ID=1086982
118 www.cnil.fr/vos-libertes/vos-droits/le-droit-dacces/
120 https://www.agpd.es/portalwebAGPD/canalciudadano/derechoscuidadano/derecho_acceso/index-ides-idphp.php
which makes it quite difficult to find out which rules his or her request should follow. Finally, the globally unsatisfactory information provided by data controllers about the right to access is another hurdle to the correct exercise of this right (cf. above section 3.1).

In this section, we analyse and assess how data subjects can concretely exercise this right, from the perspective of data controllers. To this end, we conducted interviews with the data controllers examined in the previous section.

To each data controller, we asked the following questions:
- How many demands have you received?
- Can you notice some disparities among Member States in terms of number of demands? Can you link it to the different types of forms, which are dependent upon the national legislations?
- What information is contained in the answers? Do you include what your information policies qualify as non-personal information? If so, why not?
- Do you charge?
- Any remarks, wishes for the proposed Data Protection Regulation?
- What is your approach to privacy? Do you see it as a legal burden or as a business enabler?

3.3.2 Answers to the questionnaire

Contacting the data controllers

Contacting the data controllers proved to be no easy task.

Except in the case of Wikimedia, which provides a phone number that allows user to directly contact a person dealing with privacy issues, the procedure to contact other data controllers is quite opaque. Indeed, in all the other cases, one has to talk to the customer service, which in no case was able to offer useful information. In some cases, it is possible to talk to a person, but in other cases one has to deal with an automated answering machine. One is then redirected to the legal service. However, here too no calls are taken, and one can only leave a message on an answering machine.

As far as e-mails are concerned, different situations need to be distinguished. In the case of Wikimedia, no e-mail was sent as we received satisfactory help on the phone. In the case of Google and Microsoft, luckily we knew some officers who kindly responded to our requests. However, in the cases of Amazon and Facebook, having no “inside

---

contacts”, we were left with no choice other than sending e-mails through the procedure available on the website, and which did not prove to be successful.

**Answers received**

Despite our efforts, we received no positive answers!

Wikimedia is the only data controller from whom we received an actual answer. However, they replied that to this day they have not received any demands of access.

In the case of Microsoft and Google, both of the employees whom we contacted responded; however, they were not able to provide us with some relevant information. Following these negative answers, we sent letters (both electronic and physical mail) to the legal services of these data controllers, but we have received no answers so far. And since it is impossible to reach these services by phone, one wonders what else is left to be done.

In the case of Facebook and Amazon, a letter (both electronic and physical) was sent to the legal services and/or to the EU headquarters. Yet, this did not prove to be successful.

It seems that for the ordinary citizen, entering in contact with these “big” data controllers is nearly impossible. A few possibilities are provided through dedicated procedures. That is the case for consumer feedback or press services. In some cases, specific procedures have also been foreseen to exert the right of access to data. But beyond these limited cases, the ordinary citizen seems to be in no position to ask questions relative to his or her privacy and/or to exert his or her right of access.
4 Assessment of DPAs activities on EU citizens access to personal data

Silvia Venier, Emilio Mordini (CSSC)

This chapter aims at assessing to what extent European citizens are contacting European Data Protection Authorities (DPAs) in their Member States, and complaining about difficulties in accessing their personal information or about other violations of data protection law, as well as at assessing how the supervisory authorities are handling citizens’ complaints. Generally speaking, the study also resulted in an analysis of the structure and competencies of the DPAs at the national level, as well as the DPAs’ perspectives on the recently proposed new EU data protection legal framework, in relation both to their capacity in hearing citizens’ claims and in enforcing the law.

4.1 METHODOLOGY

The research presented in this chapter has been carried out in two main phases. The first step was the analysis of the websites of the Data Protection Authorities of the 27 Member States and the European Data Protection Supervisor as well as the Art. 29 Working Party (DPAs websites inspections). The main goal was to assess to what extent the websites of the DPAs, as the most immediate and accessible communication tool, are periodically updated, providing relevant information on:

• the DPA structure and organisation: Is detailed information on DPA activities (e.g., yearly reports) available on their websites? Is there a specific department or person responsible for handling citizens’ complaints?
• citizens’ rights of privacy and data protection: Is there any documentation providing an explanation of the national data protection law? Is there any document informing citizens of their rights in this respect?
• the DPA’s activities that could help citizens to have better control over the data: Is there any activity foreseen in order to encourage citizens to gain control of or access their data? Are there any documents explaining how the DPA can support citizens’ claims? Is there any public awareness campaign in place?
• the contact procedures to notify a violation of data protection law: Are there any online forms, as well as mail addresses, telephone numbers, or any other contact details of the person in charge of hearing citizens’ notifications, available and easily accessible on the website?

The second step was to prepare a questionnaire and to send it to all Data Protection Authorities in Europe in order to collect more information on their activities. The purpose of the questionnaire was to gather contributions from European DPAs on citizens’ attitudes towards data protection, to assess to what extent EU citizens contact European DPAs and how these institutions are reacting to and supporting these claims. This touched both the question of how individual data subjects or groups of data subjects are asserting their rights as well as the more general question of whether supervisory authorities are willing and capable to enforce the law.
We proposed the questionnaire to all Data Protection Authorities in Europe, as well as to the European Data Protection Supervisor. The contacted responsible person could choose whether to answer through a short telephone interview or to reply in a written form.

The questionnaire comprises three sections (see Annex 1):
- *(Q1-Q4)* The first section focused on DPA structure and organisation, with particular reference to the effort put in hearing and investigating citizens’ complaints. It also includes a question that aimed to assess whether, in the interviewed person’s opinion, citizens are well informed about DPA activities and their data protection and privacy rights.
- *(Q5-Q10)* The second section focused on citizens’ complaints received or investigated by the DPAs, and in particular aimed to assess how are citizens addressing the DPA, whether there are specific categories of people (e.g., vulnerable groups, such as the elderly, children, disabled persons) who are excluded from this process, whether they notice, year by year, any relevant changes in the number and the types of complaints received, what are the main data protection issues at stake in citizens’ complaints, and in how many admissible complaints the DPA finds breaches of data protection legislation.
- *(Q11-Q13)* The third section aimed at assessing how the DPA is reacting to these claims, and in particular whether the DPA is able to directly reply to citizens’ complaints, whether it is experiencing any delay in replying and what is the main reason for this, how the DPA is expecting the proposed new data protection framework to impact on their activities, with particular regard to the ability to respond to citizens’ claims. This section also focused on the main co-ordination mechanisms already in place both at the bilateral and the international level.

This chapter reports the results of this study. Section 4.2 provides a general introduction on the EU Data Protection Authorities functions and activities, as foreseen by the 1995 EU Data Protection Directive and enlightening the main difficulties as well as good practices in the implementation of the provisions of the Directive. Section 4.3 reports on the main findings of the survey, in order to analyse to what extent EU citizens are contacting the supervisory authorities to notify a violation of the national data protection law and how the DPAs are reacting to these claims. Section 4.4 reports the findings of our DPAs website inspections and the results of our questionnaire survey.

### 4.2 DATA PROTECTION AUTHORITIES (DPAS) IN EUROPE

According to Art. 28 of the EU Data Protection Directive\(^\text{123}\), each Member State shall “provide that one or more public authorities\(^\text{124}\) are responsible for monitoring the application within this territory of the provisions” of the Directive. These authorities shall “act with complete independence” (Art. 28(1)) in exercising their functions and powers.


\(^{124}\)This allows for special authorities to supervise special matters.
EU Member States were bound to endow the national data protection supervisory authority with the general powers specified in:

- Art. 28 (2), i.e., power to advise legislative or administrative authorities in the process of drafting legislation or regulations relating to the protection of the individual’s rights and freedoms with regard to the processing of personal data;
- Art.28(3), i.e., power of investigation (e.g., on accessing data forming the subject-matter of processing operations), of intervention (e.g., delivering “prior-checking” opinions, before processing operations are carried out; but also issuing orders to block, erasure, destruct data), as well as of engagement in legal proceedings (i.e., to prosecute persons or organisations suspected of having violated the law);
- Art. 28(4), i.e., power to hear claims from data subjects;
- Art. 28(6), i.e., the power to co-operate with one another to the extent necessary for the performance of their duties.

In compliance with Art. 28, all EU Member States have conferred one national supervisory authority with the wide remit of monitoring the application of the Data Protection Directive.

The European Data Protection Authorities (DPAs) combine many different functions, such as informative (e.g., advising the national public bodies regarding matters related to data protection, as well as providing the data subjects with general information on their rights), administrative (in particular in respect of notification – i.e., registration of particulars of processing operations), regulatory (e.g., the duty to issue authorisation under the law), quasi-legislative (e.g., in the case of issuing codes of conduct), quasi-judicial (e.g., the consideration of applications and complaints from data subjects), as well as investigative and enforcement functions.

The implementation of the specific provisions of the Directive in the Member States has given rise to significant variations across Europe. This section gives a brief overview on the EU system of DPAs, briefly addressing major deficiencies and good practices, as well as the main changes as introduced by the recently proposed reform of the EU data protection legal framework.

4.2.1 Enforcement of the Data Protection Directive: the judicial remedy and the right to lodge claims with the national DPA

The Data Protection Directive contains various provisions aimed at ensuring the effective implementation and enforceability of the laws adopted. These fall into two broad categories: remedies that must be granted to the individuals (i.e., procedures through which data subjects can assert their rights, seeking redress and corrective actions through the courts, see Arts. 22 and 23) and the general enforcement powers.

---

125 Art. 22 Remedies reads “Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question”; Art 23 Liability “1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered; 2. The controller
that must be vested in the national Data Protection Authorities (DPAs, Art.28). According to Art. 28(4), claims can be lodged with the DPA by any person or any association representing that person, such as civil liberty organisations, consumer associations, trade unions or specialised data protection groups.

Generally speaking, the right to lodge claims as foreseen in Art. 28 can be preferred to the judicial remedy of Art. 22 as providing a cheaper, quicker and more informal redress procedure.126 When addressing the DPA, the complainant is not granted any procedural right or the right to be involved in the investigation, but merely entitled to be “informed of the outcome” of the claim. Moreover, what action a DPA can take on the basis of an individual claim, depends on the power of intervention and investigation granted to the authority by the national law, as well as on the willingness to investigate whether a violation of law is occurring. It has thus to be pointed out that the complaint procedure before the national DPA is without prejudice to the right of the data subject to a judicial remedy.

According to a 2010 Report of the EU Fundamental Rights Agency (FRA)127 on European DPAs, some divergences between the DPAs are reported with regard to the power to hear claims and engage in legal proceedings. The implementation of this function in practice may include, depending on the national DPA: a) the power to hear and review claims and complaints, b) the power to refer the case to the police of bring the case directly to judicial authorities, c) the power to make a determination itself as to the merits of the claim, d) the power to refer the matter to national parliaments.

The FRA report points out that in all Member States individuals can lodge a claim relating to a specific violation or a more general complaint before the national DPA, even if in some countries it may take an unreasonably long time for individuals to obtain information, often because many DPAs lack sufficient resources to answer all the requests received by the data subjects. Whereas all EU supervisory authorities are endowed with the authority to hear complaints, only some of them can autonomously commence legal proceedings before a competent tribunal.

With reference to the potential remedies, there are great divergences too. The DPAs can levy economic sanctions only in some Member States. Sanctions may include administrative fines imposed by the DPA, as well as criminal fines or imprisonment imposed by the judicial authority. Both economic sanctions (fines) and imprisonment are, however, extremely rare, even for obvious offences such as non-registration. Over the last few years, the DPAs in a few countries, notably in Spain, have begun to enforce

---


the law more strictly, by imposing substantial fines. In other Member States (e.g., Belgium, United Kingdom), it is common practice that the DPA negotiates amicable solutions with those found in violation.

Generally speaking, the European data protection enforcement system seems to be rather weak, and varies considerably across Member States. The absence of readably accessible comprehensive information on how the law is enforced in individual cases is also a problem: in many countries, it is difficult to get a precise view of exactly how the law is applied.

With respect to the general enforcement functions of the European DPAs, the FRA Report distinguishes two general tendencies, reflecting the approaches followed by Member States in implementing these provisions. Whereas several countries (e.g., Finland, Sweden, United Kingdom, Ireland) have mainly stressed the (ex-ante) preventive and proactive role of the supervisory agencies, other member States (e.g., Latvia, Czech Republic, Greece) have given priority to the (ex-post) enforcement and control functions. In the first cases, the preference was given to the adoption of soft preventive instruments, while in the second, to harder law enforcement measures. The majority of countries have adopted a median stand, meaning that, when a law breach is found, the authority usually first only issues a “warning” or an “advice”, and does not resort to more formal measures unless the softer ones are fully ignored by the data controller.128

To conclude, the effectiveness of the system of receiving individual complaints largely depends on three main factors: (a) the formal powers that the authorities have to act on the basis of a complaint; (b) their willingness to take forceful actions on behalf of the data subjects and against the data controllers, (c) the financial and human resources available. In practice, many DPAs tend to see themselves more as conciliators than as fierce watchdogs of data protection and privacy, usually preferring to find amicable solutions to conflicts between the controller and the data subject. This approach may give also the impression of the preference to soft and negotiable enforcement of the data protection law.

4.2.2 The power of investigation, intervention and information

Various divergences can be noticed across Europe in the implementation of other provisions of the Directive. As already mentioned, the DPAs are endowed with many different powers, that may have a deep impact on the ability to enforce citizens’ data protection rights. In this section, we briefly discuss how the powers of investigation, intervention and information are implemented in practice.

First, all DPAs in Europe are charged with investigating possible breaches of the law within their jurisdiction. According to the FRA report, the powers of investigation of European DPAs may include: (a) requesting information and documents, (b) accessing data banks and filing systems, (c) searching premises with or, in some cases, without judicial warrants, (d) conducting audits129. Such investigations can arise proprio motu

128 Ibid., p. 43
129 Ibid., p. 21
(on their own initiative) or upon request or application by a data subject who alleges violations of his personal data. When they are carried out, investigations tend to be selective, detailed and in depth.

Second, the Directive is somewhat ambiguous about the effective *powers of intervention* that must be granted to the DPA. The powers of intervention include (a) delivering prior-checking opinions, (b) ordering the blocking, erasure or destruction of data, (c) issuing a warning or reprimanding the controller.\textsuperscript{130} In addition, as already mentioned in the previous section, in many countries the DPAs can impose administrative fines. With particular reference to the system of prior checking, it is most widely developed in France for all processing operations in the public sector, but, for instance, not used in the UK. In general, there are substantial differences between the Member States in this area, as prior checking is usually seen as a fairly bureaucratic formality, very time- and person-power-consuming. In this regard, an emerging area of concern is the video surveillance cameras that are not registered in many countries, and thus not under the control of the supervisory authority.

Finally, national DPAs have also the special duty to *raise the awareness of privacy and personal data among EU citizens*. According to the 2008 Eurobarometer survey, the general public is largely unaware of its rights or of the existence and the roles of the national DPA.\textsuperscript{131} With reference to this function, with few exceptions, EU DPAs run specialised, user-friendly websites, where all relevant legislation, opinions and decisions are available and frequently updated. Art. 28(5) of the Data Protection Directive requires supervisory bodies to draw up a report of their activities at regular intervals and to make it publicly available. The Annual Reports issued by the Authorities are crucial documents in order to assess if areas of particular concerns are emerging. The DPAs advice in certain matters, as included in the reports, can be seen as an authoritative opinion in this field. The annual reports are also the documents where the national data protection “case law” is usually reported. It has to be said, however, that the overall reporting of the DPAs is not always easily accessible, structured and comprehensive. In the scope of the present study, 32 annual reports from 22 DPAs have been analysed.

### 4.2.3 Major deficiencies and good practices in the EU DPAs system

To summarise, some critical challenges can be identified for the data protection systems in the EU. The major deficiencies include the lack of independence of several DPAs, due to understaffing and lack of adequate financial resources but also because of the limited powers of the DPAs who are not endowed with full powers to investigate, intervene, offer legal advice and engage in legal proceedings.

The enforcement of data protection legislation in Member States is a major problem, with the general tendency to focus on soft methods of securing compliance with data protection legislation, instead of applying and enforcing hard instruments. This is

\textsuperscript{130} Ibid., p. 23

caused by different reasons, such as the lack of resources but also the fact that the DPAs give their enforcement actions a rather low priority, preferring conciliatory and soft measures. This may lead to a general impression that the DPAs are usually negotiating a compromise with the data controller, and that only in extreme situations seek to apply a formal sanction to data users violating the law. It is difficult to assess the true effectiveness of this approach, but it does convey the impression that data protection is minor legislation.

The lack of public awareness is another major issue. Surveys conducted at national level have found that, on one hand, the majority of EU citizens are concerned about data protection issues while, on the other, national data protection authorities are relatively unknown to them.132 Citizens are apparently not fully aware of their privacy and data protection rights. Moreover, they don’t know what are the functions of the national DPAs. As the Eurobarometer survey revealed, however, there does seem to be a general tendency across EU DPAs to strengthen public perception of the risks in this field and to make citizens aware of their rights.

With particular reference to good practices, as mentioned in the previous paragraph, these include the fact that the supervisory authorities around Europe are increasingly aware of the need to strengthen the DPA’s public awareness effort. This is one of the major areas of concern. A wide array of good practices is emerging with regard to these activities. The vast majority of DPAs have set up user-friendly, at least bi-lingual, websites where relevant information concerning data protection can be found. Through the websites, citizens may submit official complaints, and data controllers may request and receive advice in processing operations. DPAs regularly make available their activity reports on the websites. The educational policy devised by some DPAs (see for instance the Czech Republic DPA’s program “Protection of Personal Data in Education”, or the internships programs run by the DPAs in Portugal and Belgium133) is another innovative element, and includes the provision of educative programs at all levels of the national scholastic system, a wide offer of guidance and advice related to specific data protection fields, as well as, in some countries, the establishment of special prizes to be awarded by the DPA134.

Another good practice might be seen in the degree of co-operation with other institutions as well as privacy advocates and civil society organisations. Generally speaking, European DPAs have established co-operation mechanisms with three different categories of stakeholders, i.e., state institutions, NGOs and DPAs of other Member States. Good practices emerge when DPAs are able to sign ad hoc memoranda or co-operation agreements with other public institutions, such as the police or other Ministries.

At the EU level, the national supervisory authorities co-operate and work jointly with each other under the framework of the Art. 29 Working Party. The working group, established according to Art. 29 of the Directive, provides for the necessary institutional

132 Ibid.
134 Ibid., p. 49.
environment for DPAs to harmonise the application of their respective laws. The opinions and recommendations of the working party have contributed to the development of a common EU standard with a high level of personal data protection.

4.2.4 The new data protection legal framework and the enhanced role for DPAs

This study has been conducted in a period of profound change for the European Union DPA system. The Lisbon Treaty (see Art. 16 TFEU) opened the opportunity for the EU to strengthen and widen its data protection regime. Data protection in Europe is enshrined as an autonomous human right in the EU Charter of Fundamental Human Rights (Art.8), which now enjoys the same legal value of the Treaties. The Lisbon Treaty also abolished the pillar structure.

The need to strengthen the role of the Data Protection Authorities emerged over the past decade as a priority in order to ensure the enforcement of the principles of the Data Protection Directive throughout Europe. On 4th November 2010, the European Commission published a Communication on “A comprehensive approach of data protection in the European Union”135 which set out the main themes of the foreseen reform of the data protection legal framework in the EU. Among other initiatives, the Commission stated the importance to strengthen the DPAs’ independence and powers, so that they are properly equipped to deal effectively with complaints, with powers to carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions. In the EC communication, the need to provide the DPAs with “the necessary powers and resources to properly exercise their tasks both at national level and when co-operating with each other” emerged as a key issue in guaranteeing respect for data protection. The Commission particularly emphasised the need to properly implement the concept of “complete independence” for the European DPAs, as well as to improve the co-operation and co-ordination mechanisms at the EU (i.e., through the Art. 29 WP and the EDPS) and at the bi- or multi-lateral level.

The recently proposed reform of the Data Protection Directive introduced new developments for the DPA regime. The proposed Regulation, that should replace Directive 95/46/EC, aims at reducing the fragmentation of legal regimes across the 27 Member States and providing legal certainty by introducing a harmonised set of core rules.136 This will have important impacts on EU DPAs, as summarized in the EC Communication accompanying the legislative proposal137 as follows:

• To further enhance the independence and powers of national data protection authorities to enable them to carry out investigations, take binding decisions and impose effective and dissuasive sanctions;
• To oblige Member States to provide them with sufficient resources;

• To set up a “one-stop-shop” system, through which data controllers in the EU will have to deal with a single DPA (i.e., the DPA of the Member State where the company’s main establishment is located);
• To create the conditions for the swift and efficient co-operation between DPAs, including the obligation for one DPA to carry out investigations and inspections upon requests from another, and to mutually recognise each other’s decisions;
• To set up a consistency mechanism at EU level to ensure that DPA decisions that have a wider EU impact take full account of the views of other DPAs concerned, and are fully in compliance with EU law;
• To upgrade the Art. 29 Working Party to an independent European Data Protection Board, in order to improve its contribution to consistent application of data protection law and to provide a strong basis for co-operation among data protection authorities, including the European Data Protection Supervisor, that will provide the secretariat of the Board.

Chapter VI of the proposed Regulation is devoted to the Independent Supervisory Authorities. Section 1 sets out rules for their independent status, clarifying the conditions for their independence. Section 2 sets out the rules on their duties and powers, that include the powers of hearing and investigating citizens’ complaints, sanctioning administrative offences and promoting public awareness. Chapter VII of the Regulation, Co-operation and consistency, deals with co-operation mechanisms (section 1) to be put in place at the bilateral and European levels, with the rules for a consistency mechanism for ensuring unity of application in relation to processing operations (section 2), while section 3 establishes the European Data Protection Board, which will replace the Working Party and will consist of the heads of the EU DPAs and of the EDPS, who will provide the Board’s secretariat. Chapter VIII on Remedies, Liability and Sanctions, provides the right of any data subject to lodge a complaint with a supervisory authority (Art. 73), the right of a specific judicial remedy against the supervisory authority, that obliges the authority to act on a complaint (Art. 74), the right of judicial remedy against a controller or a processor (Art. 75), the right to compensation (Art. 77). It obliges Member States to lay down rules on penalties and to sanction infringements (Art. 78), and DPAs to sanction the administrative offences listed in the catalogues set out in this provision (Art. 79).

Question 12 of our questionnaire, sent under the scope of this research, was aimed at gathering information on how EU DPAs are expecting the proposed reform to impact on their daily activities, with particular reference to the handling of complaints from citizens, as well as on co-operation and collaboration with other DPAs and at the EU level.

4.3 SURVEY ON HOW EU DPAS ARE HANDLING CITIZENS’ COMPLAINTS

This section outlines the findings of the survey on how citizens are addressing their national DPA and how the authority is reacting to citizens’ claims and handling citizens’ complaints. The following paragraphs report on the analysis of the DPA activities in each Member State, both resulting from the inspection of their websites and analysis of their annual reports, as well as from the interview questionnaire (when available).
The survey questionnaire (see Annex I) was sent to all DPAs in Europe. A reminder was also required in order to solicit a reply and was sent two weeks after the first e-mail. Two options were provided to contribute, i.e., the possibility to schedule a short telephone interview or to reply in a written form. Out of 27 Member States and one EU institution (EDPS), 19 Authorities replied to the questionnaire, i.e., the European Data Protection Supervisor and the DPAs of Belgium, Cyprus, Czech Republic, Denmark, Estonia, Italy, Ireland, Germany, Latvia, Luxembourg, Netherlands, Portugal, Slovakia, Slovenia, Spain, Sweden, UDL (DPA of the German Land Schleswig-Holstein), United Kingdom (see Annexes II and III). One DPA (Lithuania) sent an official reply explaining that, due to the large number of cases in progress and complaints received, they were not able to contribute. When responses to the questionnaire were not available, the main sources of information have been a DPA’s website and annual reports (when available in English).

The results of this research are analysed and discussed in the following paragraphs. The conclusions are reported in the last section of this chapter.

**4.3.1 European Data Protection Authority**

*About the institution*

The European Data Protection Supervisor (EDPS) is an independent supervisory authority established in 2004 in accordance with Regulation (EC) No 45/2001. Based in Brussels, the EDPS is in charge of supervising the processing of personal data by European institutions and bodies, of advising EU institutions and bodies on all matters relating to the processing of personal data including advice on legislative proposals, and of co-operating with national supervisory authorities, in particular, as concerns the former “third pillar” of the EU.

Information and communication play a key role in ensuring the visibility of the EDPS’ main activities and in raising awareness both of the EDPS’ work and of data protection in general. The EDPS runs a user friendly and frequently updated website[139](http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en), which is the most important communication channel and information tool. The annual reports, the EDPS "key publication"[140](http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en), are available on the website. With regard to the effectiveness of the institutional communication strategies and public awareness campaigns, the EDPS is currently undertaking a survey to understand the perception of the European stakeholders on their activities. Intermediate results indicate that civil society generally knows EDPS activities (for about 20%, it is very well known and for 40%, well known). The results of this survey will help the EDPS to develop an internal strategy plan. Once finalised, a final report on the strategic plan will be made public.

*About the complaints received*

According to the EDPS 2010 Annual Report:

---

[138] Main sources for this section: EDPS website, EDPS Annual Reports, Questionnaire
In principle, an individual can only complain about an alleged violation of his or her rights related to the protection of his or her personal data. Only EU staff can complain about an alleged violation of data protection rules, whether the complainant is directly affected by the processing or not. [...] According to the Regulation, the EDPS can only investigate complaints submitted by natural persons. Complaints submitted by companies or other legal persons are not admissible.\textsuperscript{141}

In December 2009, the EDPS adopted an internal manual designed to provide guidance to staff when handling complaints. The EDPS has also implemented a statistical tool designed to monitor complaint-related activities.

The handling of individual complaints, however, constitutes a small part of the EDPS activities. A precise indicator on how much time is spent on this activity is not available, but according to the survey respondent, it is probably less than 5%. The EDPS is not noticing any clear pattern in the number and type of complaints received since 2008. According to the EDPS Annual Report, in 2010, the complexity of the received complaints increased, while the number slightly decreased with respect to 2009\textsuperscript{142}. In 2010, the EDPS received 94 complaints (a decrease of 15% compared to 2009). Of these, 69 complaints were inadmissible, the majority relating to processing at national level as opposed to processing by an EU institution or body. The remaining 25 complaints required more in-depth inquiries. Of the admissible complaints submitted in 2010, the majority (80%) were directed against the European Commission, including the European Anti-Fraud Office (OLAF) and the European Personnel Selection Office (EPSO).

The main issues involved breach of data subjects’ rights, such as access to and rectification of data or objection and deletion, violation of confidentiality and excessive collection of personal data. According to the EDPS, only in about 5-10% of admissible cases\textsuperscript{143} is a persistent breach of data protection rules found. In some cases, the data controller corrects the breach during the inquiry at the EDPS request.

Among the main tools to contact the DPA, e-mail is most commonly used. Since 2011, the EDPS implemented an online submission form which is now often used. Postal correspondence or telephone are rarely used. In simple cases (such as non-admissible cases or simple requests of information), the EDPS usually replies within one or two weeks. Complex investigations require a longer period, and in some exceptional cases, can take even two or three years.

\textit{About the new data protection framework reform and the collaboration mechanisms}

According to the EDPS, the proposed reform does not affect the rules under which the institutions works. EDPS competence and tasks in respect of EU institutions and bodies and claims from individuals against them will remain as before under the terms of Regulation (EC) No 45/2001. The EDPS will, however, be more involved in the resolution of trans-border claims from individuals against controllers who are not EU

\textsuperscript{141} Ibid., p. 30.
\textsuperscript{142} Ibid., p. 33.
\textsuperscript{143} The complaint is, in principle, \textit{inadmissible} if the complainant has not first contacted the institution concerned in order to redress the situation. If the institution was not contacted, the complainant should provide the EDPS with sufficient reasons for not contacting it.
institutions when they fall under the “consistency mechanism”. In such cases, the complaint would be dealt with through the European Data Protection Board (EDPB), in which the EDPS will participate as member and for which it will also provide the secretariat. As host of the secretariat, the EDPS will have an increased role in facilitating the co-ordination of supervisory authorities to respond to claims made through the consistency mechanism.

Co-ordination and collaboration mechanisms are to some extent already in place under Directive 95/46/EC, Article 29 of which set up a working party composed of all the EU data protection authorities. The Article 29 Working Party contributes to ensuring consistency in the interpretation of Directive 95/46/EC within the EU. Furthermore, in the field of ex third pillars system (i.e. in the Schengen Information System, SIS, in the Visa Information System, VIS, etc.), co-ordinated supervision is done by the EDPS together with national DPAs.

### 4.3.2 Austria

#### About the institution

The Austrian Data Protection Commission is the Austrian supervisory authority for data protection. It is based in Vienna and was established in 2001, after the entry into force of the Austrian Data Protection Act. The Commission is responsible for issuing recommendations on data protection matters and gathering requests of notifications, but can also file a lawsuit before the competent court of law in case of severe transgressions.

The main website of the authority is in German, while a less detailed version is run in English. The website contains information on the legal texts, both at the national and international level, as well as a list of hyperlinks to the EU DPAs and information on data security. A newsletter is also available on the website, and covers the period from 2006 to 2008.

#### About the complaints received: No information was available.

#### About the new data protection framework reform and the collaboration mechanisms: No information was available.

### 4.3.3 Belgium

#### About the institution

The Belgian DPA, the Commission de la protection de la vie privée, was established by the Belgian Federal House of Representatives with the Belgian Act of 8 December 1992. It is assisted by a secretariat. As of 1 January 2004, the Commission has been an independent supervisory authority under the auspices of the Belgian House of Representatives. The Commission’s mission is to ensure that privacy is respected when

---

144 Main sources for this section: DPA website https://www.dsk.gv.at/DesktopDefault.aspx?alias=dsken
145 See the PRIVIREAL website at http://www.privireal.org/content/dp/austria.php
146 Main sources for this section: DPA website, DPA Annual Report, Questionnaire.
personal data are processed. Within the Commission, sector committees have been established, which are in charge of supervising a specific sector.

The Commission consists of 16 members: a president, a vice-president, six permanent members, eight substitute members. The President and Vice-President are the only members occupying a full-time position. The President's position is occupied by a magistrate. The Vice-President's mother tongue always has to be French when the President is a native speaker of Dutch, or vice versa. Commission members must include at least one legal counsellor, one IT specialist and two individuals with experience in personal data management, in the public and private sector respectively. The 16 Commission members are all designated for a renewable six-year term. Every one of them, in his or her own way, is an expert in the protection of privacy and personal data management.

According to the questionnaire respondent, the Commission informs citizens mainly through the DPA website and responding to questions from the press. No studies are currently planned in the context of assessing citizens’ awareness of the activities of the supervisory authority. The yearly reports, a legal obligation for this DPA, are available on the website.¹⁴⁷

*About the complaints received*

The Belgian DPA has a specific office for first-line help dealing with complaints and requests for information made by citizens. There also is a legal department handling complaints requiring more research and requests for opinions coming from the legislator.

The object of complaints often depends on current events. Last year, for instance, Google Street View was launched in Belgium, which caused a peak in the complaints and requests for information addressed to the Belgian DPA. Other recurring topics are surveillance cameras, credit registration, press freedom, police and justice, the employer/employee relationship and direct marketing.

The DPA has a contact form on its website, but contact is also possible by letters or through e-mail or a call to the first-line help desk. Citizens often address the DPA to request information on their rights, to send a complaint about press articles or photos, mainly related to the right to be forgotten, to request access to their data in police databases. According to the annual report, the DPA on average finds breaches of the data protection legislation in 5.9 % of all complaints received. The authority replies to citizens directly, respecting internal deadlines established by service level agreements.

*About the new data protection framework reform and the collaboration mechanisms*

In the authority’s perspective, the data protection reform will give the DPAs the power to impose sanctions as opposed to their current “power of mediation”. Another important change will be the abolition of the notification system, which will reduce the DPA administrative workload. There may be a higher workload, however, related to the technical analysis of data breaches, which would have to be notified to the DPA under the proposed data protection regulation.

Moreover, the new regulation introduces the concept of a “one-stop shop” for controllers, meaning that data subjects can still address their national authority for problems with a controller, but it will be the DPA of the country where the controller’s main establishment is located that will deal with the complaint at the request of the DPA to which the complaint was submitted.

The current EU Data Protection Directive provides for co-operation between DPAs. This cooperation is not official but informal and depends on the willingness of other DPAs to respond to the requests as well as their workload. An official co-operation mechanism is the one established for the Binding Corporate Rules, i.e., for cross-border data transfers by multinationals, which, according to the authority, works very well.

4.3.4 Bulgaria

About the institution

The Bulgaria Commission for personal data protection is an independent supervisory authority based in Sofia. It is a collegiate body, consisting of a Chairman and four members, elected by the Parliament for a period of five years with a possibility to be re-elected for five years more. The Commission is supported by an Administration divided into four departments: Finances and International Activities, Software and Hardware Department, Information Department and Legal Department. The total number of employees is 71.

The Commission should submit an annual activity report to the Parliament and the Council of Ministers. The Commission’s tasks are to analyse and exercise overall control on the compliance with the legislation in the field of personal data protection, to keep a register of personal data controllers, to inspect the controllers’ activities, to give opinions and permissions in the cases covered by the Act, to issue obligatory instructions to controllers, related to the protection of personal data, to impose temporary suspension on personal data processing that breaches the personal data protection rules, to review complaints against controllers who have refused persons access to their personal data as well as other controllers’ or third parties’ complaints in relation to their rights under the Act, and to participate in the drafting of legislation containing provisions on personal data protection.

About the complaints received: No information was available.

---

About the new data protection framework reform and the collaboration mechanisms: No information was available.

4.3.5 Cyprus

About the institution

The Office of the Commissioner for Personal Data Protection was established in 2001 in Nicosia\(^{149}\). Within the functions of the Commissioner for Personal Data Protection is the supervision of the application of the law and the observance of the principles for the protection of personal data. The main functions of the Commissioner’s Office relate to the examination of notifications which are submitted in respect of the establishment and operation of filing systems, the issue of licences for the combination of filing systems and for the transmission of data to third countries, the inspections of filing systems and the investigation of complaints.

On the English version of the DPA’s website, one can find information on the country’s legislation on the protection of personal data, links to national institutions and other EU DPAs, as well as the “Year Review Reports”. The Greek version of the website is frequently updated and includes more comprehensive documentation, as well as an online contact form.

About the complaints received

According to the 2009 yearly report, the number of complaints submitted in that year was 348. This number increased by 26% compared to the previous year. The majority of complaints submitted (73%) referred to unsolicited communication, commonly known as “spam” or “junk mail” or “commercial junk mail”. The number of this type of complaints is growing every year in Cyprus\(^{150}\).

Other complaints concerned unauthorised or excessive disclosure of personal data, most of the time from one organisation or public authority to another. Interestingly for the present research, in 2009, there was an increase in the number of complaints received by individuals for non-satisfaction of their right of access to their personal data. Most of these complaints received full satisfaction. The right of access was also a main topic of discussion during the 20th Complaints Handling Workshop, organised by the Office of the Commissioner in Limassol in October 2009.\(^{151}\)

According to the respondent, in Cyprus, they are witnessing a small increase in the number of complaints regarding the Internet and video surveillance. They are not observing any particular patterns in the categories of people that are filing complaints in general, but it is evident that most of the complaints regarding the Internet are submitted by younger people.

\(^{149}\) [Link](http://www.dataprotection.gov.cy) Main sources for this section: DPA website, DPA Annual Report, the survey questionnaire.


\(^{151}\) Ibid., page 11
According to the general rules of the administrative procedures, the DPA, before reaching a conclusion / issuing a decision on a case, has to give the other party the right to express its opinion and comment on the allegations (one month period is given to the other party to reply). In cases where a breach of the law is found, the other party is also given the opportunity to state any reasons why a fine should not be imposed. For this, another month period is given. Also, there is a delay in replying in many cases where the DPA needs to obtain information from third parties (e.g. ISPs or banks).

**About the new data protection framework reform and the collaboration mechanisms**

According to the respondent, they are not in the position of estimating the impact of the proposed reform at this stage. Collaboration mechanisms are already in place such as the Article 29, case-handling workshop, Contact Network of Spam Authorities (CNSA), International Working Group for Data Protection in Telecommunications.

**4.3.6 Czech Republic**

**About the institution**

The Czech Republic DPA was established in 2000 by the Consolidated Version of the Data Protection Act, as an independent governmental body. The Authority is based in Prague. With reference to its competencies, they are specified primarily in the provisions of Art. 29 of the Data Protection Act. The authority can comment the drafts of legal acts and regulations, and send its comments to the responsible ministries (legislative competence). Other competencies include the recording of notifications (administrative function), the overall supervision of data processing in the public and private sectors, and the imposition of remedial measures (supervisory function), as well as the acceptance of complaints from citizens and the public-awareness-raising-related activities.

Since the DPA’s comments on the national census carried out in 2000, the institution has been experiencing a great media coverage. According to the person interviewed in the scope of the present study, in Czech Republic the public is well informed about data protection rights and about specific activities of the national DPA. Specific public awareness campaigns are also foreseen in the future. As stated in the 2010 annual report, the office will "control, more consistently than today, measures of a preventative and awareness raising nature, with the aim to further improve the legal awareness of personal data subject".

The website of the Czech Republic DPA is the authority’s most important communication channel. It is a comprehensive repository of legal documents, position papers, informative reports on selected issues, that include unsolicited commercial...

---

152 Main sources for this paragraph: DPA website, DPA Annual Reports, Telephone Interview
communications, the Schengen Information System, and a comprehensive guidance for entrepreneurs. The website is constantly updated with relevant news. The Annual Reports are available on the devoted section of the website\textsuperscript{157}.

About the complaints received

The Czech Republic Data Protection Act includes special provision concerning citizens’ complaints. The authority has a special department devoted to negotiation with the public, and a special unit that replies to complaints.

According to the interviewed person, a progress in the number and different types of complaints received can be noticed in the last years. In 2010, for the first time during the existence of the office, the DPA received more than 1,000 complaints about illegal conduct in personal data processing: as mentioned in the 2010 annual report\textsuperscript{158}, over the last 5 years, the number of complaints received has increased almost three-fold, which has required the adoption of corresponding measures, particularly as regards the stuff.

The main sectors concerned are: video surveillance in public spaces, surveillance at work (in this case the competences is shared with the Labour inspector), and online services (with this respect, the main problem is related to the fact that the complaints are based on data controllers that are outside the EU).

In the respondent's opinion, there is not any particular relevance in the categories of people who are addressing the DPA. In particular, it is noticed that the elderly are not addressing frequently the DPA, since they don’t seem to be educated in recent data protection legislation. Minors need to be accompanied by an adult to send their complaints.

The complaints are submitted to the DPA though telephone, email and paper. On the authority website, there are also specific forms to report on SPAM and data breaches in the telecommunication sector. The majority of claims posed by the citizens include the data controllers’ right to collect data, the accuracy of the data, as well as the penalties of specific data breaches.

Generally speaking, it can be said that the DPA department responsible for hearing citizens’ claims usually find data breaches in 1/3 of the submitted complaints. The DPA is not experiencing any delay in replying. According to the Czech Procedural code, replies have to be sent within a month, but the DPA usually reply within a number of days a couple of weeks. In the case of particular complex complaints, i.e. above all when there is the need to contact other ministers or foreign DPA, the overall process may require a longer period of time.

About the new data protection framework reform and the collaboration mechanisms


In the respondent’s view, the new reform of data protection may result in establishing stronger communication channels between all national DPAs, that may result in enhancing enforcement procedures. Better cooperation and coordination mechanisms with other DPA will be provided by better regulation in this area. It will be possible to exactly and immediately know which DPA is responsible for handling a particular case, and the art 29 WP will be promoted into the EU “data protection board”. With regard to the expected positive outcomes of the new data protection reform, the respondent mentioned also the obligation to set up a DPO for large companies, that will mean to have one, competent person who will be responsible for dealing with the DPA.

4.3.7 Denmark159

About the institution

The Act on Processing of Personal Data entered into force in 2000 and is under the authority of the Danish Data Protection Agency. The authority competencies cover the duty of providing guidance and advising other public sector bodies, supervising the private sector companies, as well as hearing citizens complaints. According to the respondent, 20% (estimated) of the total resources allocated to the Danish DPA are currently devoted to this last function.

The authority runs a complete and user friendly website, that includes all relevant documentation. The Annual reports are available only in Dutch and are uploaded into the devoted section of the website. According to the respondent, Dutch citizens are increasingly aware of their data protection and privacy rights. However, not all know about the DPA’s activities. No study is planned at this point on how to raise citizens’ awareness.

About the complaints received

According to the respondent, the number of complaints and questions received by the Dutch DPA has doubled from 2007 to 2012. Most dominant sectors regards the Internet/social networks, credit agencies, the telecommunication and the financial sector, as well as data protection in employment procedures, and the Danish identification number. Phone calls and emails are the most commonly used tools by citizens. Citizens address the DPA in order to request information, to ask what are their rights in a specific case and to report alleged violations.

About the new data protection framework reform and the collaboration mechanisms: No information available. According to the respondent view, it is too early to comment on this issue.

4.3.8 Estonia160

---

159 Main sources of this section are: the DPA website, the Questionnaire.
160 Main sources of this section are: the DPA website, the 2010 Annual report, the Questionnaire.
About the institution

The role of the Estonian Data Protection Inspectorate is to defend the following constitutional rights: the right to obtain information about the activity of public agencies, the right to inviolability private and family life in the use of personal data, and the right to access data gathered by data controllers. Major efforts are also put into raising awareness in the fields of personal data protection and transparency of public sector.

The Annual Reports are available on the dedicite section of the authority website. The Introduction to these reports is translated into English. No study on the need to establish further public awareness raising campaigns has been carried out recently. According to the respondent’s view, however, “as the amount of complaints is increasing, this should mean that the amount of informed citizens should also be increasing”.

About the complaints received

General statistics on the complaints received by the Estonian DPA are available on the authority website. The number of calls received reached the 1,000 in 2010, while the complaints are increasing since 2009. Citizens are contacting the DPA mainly through e-mail and phone calls (the authority has set up a dedicated help-line), in order to report violations of the data protection law (denial of access to personal data is also considered as a violation), or to ask information on their rights.

About the new data protection framework reform and the collaboration mechanisms

Joint inspections are carried out particularly with DPAs of the Baltic States. No further information is available on the expected impact of the data protection reform. According to the respondent view, it is too early to comment on this issue.

4.3.9 Finland

About the institution

There are two data protection authorities in Finland: the Data Protection Board (DPB) and the Data Protection Ombudsman (DPO). The DPO is appointed by the Council of State for a term of 5 years. He has a preventive and guidance-oriented role, and operates in connection with the Justice Ministry. The DPB consists of a chair, deputy chair and five members, who are required to be familiar with register operations. The Board is appointed by the Council of State for a term of three years. The Data Protection Board processes and makes decisions on issues falling within its scope of action such as supervision, inspection, information and international cooperation. At the request of the

---

162 See the questionnaire compiled on behalf of the Estonian DPA available in Annex III.
163 http://www.aki.ee/eng/?part=html&id=146&PHPSESSID=i7427rt7d1rsmu0477o80rl7v0
164 Main sources of this section are: the DPA website, the Annual Reports
Data Protection Ombudsman, the board provides regulations concerning the processing of personal data.

The Finnish data protection authority has established an updated and comprehensive website, with relevant documentation on the legislation and other activities of the DPA, where the yearly reports can be also downloaded.\(^{165}\)

*About the complaints received:* No information was available

*About the new data protection framework reform and the collaboration mechanisms:* No information was available

### 4.3.10 France\(^{166}\)

*About the institution*

The French Commission National de l'Informatique et des Libertés (CNIL) is the country's authority responsible for the implementation of the data protection law. It has been established in 1978. New legislation on data protection was introduced in August 2004. The CNIL is composed by a college of 17 personalities\(^{167}\), among whom there are members of the national Parliament and representatives of the country's highest Courts.

The competencies of the commission are to inform citizens and assist individuals in the exercise of their rights, with particular attention paid to the right of access to the personal data, to advice public bodies and to adopt regulations for a correct implementation of the law, to keep an inventory of current processing operations, to supervise compliance with the law through investigations and on the spot inspections.

The CNIL website is a very user-friendly communication tool that is constantly updated and includes relevant information on legislation as well as dossiers on specific topic, such as biometrics, video surveillance, data transfers, internet and surveillance at work\(^{168}\). The website is available in French, English and Spanish. The yearly reports ("rapports d'activité") are also available in the dedicated section of the portal\(^{169}\). A big part of CNIL’s effort is also devoted to the promotion of regular public awareness campaigns.

*About the complaints received*

In addition to the guidance, supervision, audits and information functions, the CNIL is also responsible of handling citizens complaints related to alleged violations of the data protection law. According to the 2010 annual report, in that year the commission received 4,821 complaints, out of which 1,877 were requests of accessing data collected about them by the law enforcement authorities (the so called “demandes de droit


\(^{166}\) Main sources of this section are: the DPA website, the Annual Reports

\(^{167}\) See [http://www.cnil.fr/english/the-cnil/status](http://www.cnil.fr/english/the-cnil/status)

\(^{168}\) [http://www.cnil.fr](http://www.cnil.fr)

d’accès indirect”). This number represent an evident increase (13%) with respect to 2009\textsuperscript{170}.

In June 2010, the CNIL launched also the service “plaints en lignes”, which could help explaining the increase in the number of complaints received that year. Nowadays, 20% of the complainants are using Internet to address the institution.

Citizens complaints were mainly related to the following sectors: banking and financial sector, unsolicited commercial communication, online services (e.g. complaints related to the right to be forgotten), the telecommunication sector and surveillance at work. Video surveillance in public spaces and the issue of the “droit à l’oubli” over the internet are the areas witnessing the stronger increase of number of complaints.

In the 20% of cases, the authority is in the position to directly reply to citizens complaints, to their requests of information or when the CNIL is not competent over a case. In the 80% of complaints, the CNIL has to contact the data controller in order to investigate the alleged violation of data protection law\textsuperscript{171}. On-the-site controls are also possible, as well as the issuing of administrative sanctions, that, however, usually happens only in the 2% of cases. The period of time required to reply to citizens’ complaints may vary from a couple of days to some months, depending on the complexity of the enquiry and on the collaboration willingness of the data controller.

*About the new data protection framework reform and the collaboration mechanisms*

Relevant information on the international activities of the CNIL is available on the dedicated section of the website\textsuperscript{172}. No information on the expected impact of the new EU data protection reform on the CNIL activities is available.

4.3.11 Germany\textsuperscript{173}

*About the institution*

The Federal Commissioner for Data Protection and Freedom of Information is elected by the German Bundestag. His legal position and his task are laid down in the Federal Data Protection Act (BDSG). According to this Act he is independent in the performance of his duties and only subject to the law. This means for example that in connection with the performance of his duties, the Federal Government is not entitled to give him any instructions with regard to the subject matter. The Federal Commissioner is only subject to the legal supervision of the Federal Government and only with regard to issues relating to service law he is subject to the administrative supervision of the Federal Ministry of the Interior. All public federal bodies are obliged to support him and his staff for the performance of their duties.

The Federal Commissioner’s main tasks include first the provision of advice to the German Bundestag. The Federal Commissioner impartially provides the German

---


\textsuperscript{171} See the CNIL Annual Report 2010, page 14

\textsuperscript{172} See http://www.cnil.fr/la-cnil/nos-defis

\textsuperscript{173} Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
Bundestag with expert knowledge about all developments in the field of data protection and gives recommendations when and by which laws or other measures the German Bundestag should intervene in the development. In addition, the Federal Commissioner advises the Federal Government, all public federal bodies and other bodies (cf. Sect. 26 BDSG). Moreover his tasks include controls (cf. Sections 24, 25 BDSG) and cooperation in matters relating to data protection law at the European and at the international level.

The Federal Commissioner has extensive investigative powers. Admittedly, he is not entitled to give instructions. However, when the Federal Commissioner has detected a data breach he has the possibility to report this violation to the law enforcement authorities and to lodge a demand for prosecution.

Another main task of the Federal Commissioner is the dealing with requests by petitioners: anyone who believes his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies of the Federation may appeal to the Federal Commissioner (Sect. 21 BDSG).

In addition, the Federal Commissioner is responsible for monitoring the direct federal social insurance institutions, telecommunications- and postal service companies and private companies falling within the Security Clearance Check Act.

Informing the public is one of the Federal Commissioner's main tasks. Every two years the Federal Commissioners publishes an activity report in which he informs the German Bundestag and the public about essential developments in the field of data protection and about the focal points of his tasks. The activity report is ready for download on his website174. In addition to the activity report the public is also informed by active public relations work.175

Public administrative bodies of the Federal States and/or of local governments are monitored by the data protection commissioners of the Federal States. So-called non-public bodies such as companies are subject to the data protection supervisory authorities for the non-public area of the Länder. Their tasks also include the dealing with petitions within their field of responsibility. Also these data protection supervisory authorities have extensive investigative powers.

About the complaints received

In 2011, among the whole documents the Federal Commissioner received, the amount of petitions was 25%. According to the questionnaire respondent, the amount of written complaints and requests at the Federal Commissioner’s has nearly tripled in the last five years. The number rose from 2.449 requests in 2005 to 6.087 in 2010. As a whole, in this

---

174 [http://www.datenschutz.bund.de](http://www.datenschutz.bund.de)
period, about 24,000 citizens appealed to the BfDI in writing. In addition, there are approximately 7,000 telephone calls per year. 176

In 2011 the Federal Commissioner received for the first time more requests by telephone than in writing. Admittedly, in 2011 “only” 5,161 citizens appealed in writing to the Federal Commissioner, but more than 9,000 requests for advice were received per telephone.177

There is no statistical information available on the main categories of people who are more frequently addressing the Federal Commissioner. In addition to general information the petitioners often wish the Federal Commissioner to take action against the data controller. Most of the requests concern the topics of data protection in the non-public sector, health and social issues, telecommunications- and postal services.

About the new data protection framework reform and the collaboration mechanisms

According to the respondent’s view, in general there is no additional impact expected of the new reform in their daily activities, as the Draft Regulation does not deviate too much from the German Data protection legislation. When the respective request would be of a border over spilling interest, the newly developed “consistency mechanism” could apply (Art.57, 58). But the Art. 29 Working party and the subgroups consults on likewise matters also now most thoroughly, while the procedures are not yet that formalised.

4.3.12 Germany – State of Schleswig-Holstein178

About the institution

The Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD, English: Independent Centre for Privacy Protection) is the Data Protection Authority of Schleswig-Holstein, the northernmost Federal State of Germany. Its office with 40 employees is located in Kiel, Germany. The ULD is responsible for supervision of both data protection and freedom of information in Schleswig-Holstein.

The basis for the work of ULD is laid down in the State Data Protection Act Schleswig-Holstein (LDSG S-H). This act is one of the most progressive ones worldwide and includes among others provisions on a seal of privacy for IT products and on privacy protection audits for public authorities. In addition to the privacy seal based on German national and regional law, ULD is coordinating the European Privacy Seal Initiative EuroPriSe, which grants privacy seals on the European level in case of a successful evaluation of compliance with European data protection regulation.

The LDSG S-H only covers the supervision of the public sector; for the private sector the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) has to be applied. The

---

177 Ibid.
178 Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
freedom of information tasks are laid down in the Freedom of Information Act Schleswig-Holstein (Informationszugangsgesetz – IZG).

Since 1998 ULD has been working on several national and international projects in the field of data security and privacy protection, among others, the EU-funded IST projects “FIDIS – Future of Identity in the Information Society”, “PRIME – Privacy and Identity Management for Europe”, “PrimeLife”, “ABC4Trust – Attribute-based Credentials for Trust”, and “TClouds – Trustworthy Cloud Computing”.

The ULD is organised into 7 departments that are: Dep. 1: service area: organisation of the office, human resources, public relations; education: data protection training courses; Dep. 2: fundamental legal questions on data protection in the public sector, data protection in the areas of government, tax, schools and universities, social matters, medicine etc.; freedom of information; Dep. 3: fundamental technical questions on data protection and privacy technologies, data security, system data protection, technology and media; support of the other departments; Dep. 4: data protection in the private sector, e.g., trade, banking and assurance, associations, address trade and inadmissible advertisement, market and opinion research, video surveillance, employee data protection, internet, geo data, scoring; Dep. 5: data protection in the areas of police and justice; Dep. 6: coordination of studies and projects for privacy by design, e.g., PrimeLife, ABC4Trust, TClouds; cooperation issues; privacy research; Dep. 7 (I): ULD privacy seal; data protection audits; Dep. 7 (II): EuroPriSe – European Privacy Seal; data protection on the international level. Dep. 2, 3, 4 and 5 are active in investigation, consulting, auditing, and enforcement for their respective subject-specific areas.

Until 2011, ULD regularly provides a yearly report. In the last revision of the LDSG S-H, a report per every two years is foreseen which will cover the years 2011 and 2012. This report will be presented in the beginning of 2013.

According to the respondent, the citizens living in Schleswig-Holstein are well informed on several of ULD’s activities because of a regular press coverage (newspapers, radio and TV broadcasts, magazines) and information via the ULD website, subscriptions to our mailing lists etc. ULD’s press releases are quite well taken up by the press. Further, journalists from Schleswig-Holstein and beyond ask for comments and statements on privacy and data protection (usually multiple times per day). “This does not mean that all facets of ULD’s work are well known by all citizens”, but rather that, regarding the possibility to complain, many people address ULD (even if ULD is not responsible).

Moreover, ULD is hosting the Virtual Privacy Office that provides the website/portal of “www.datenschutz.de”. This is regarded as an entry point for German (or German speaking) internet users who are interested in privacy and data protection.

About the complaints received

All citizens’ complaints are taken seriously and are investigated. The effort is dependent on the number of citizens’ complaints because the employees in the supervision part of

ULD also regularly schedule general supervision visits in the public and in the private sector that are independent from individual complaints.

According to the respondent’s view, it can be stated that the amount of complaints has increased. With reference to the major sectors involved, many complaints involve data protection on the internet (including advertisement, marketing, e-commerce, personal data put online by others) or video surveillance in public spaces. The number of complaints regarding employee data protection has also increased (not only surveillance at work). Data protection in the social sector has been a hot issue for years, but meanwhile ULD is not in charge of tackling those complaints anymore because this task has been shifted to the Federal Data Protection Commissioner. Eventually, cases in the medical sector play a bigger role. Quite regular are complaints because of non-shredded medical files in trash bins.

With regard to the information on categories of citizens addressing the DPA, in many cases no specific assessment can be done. There has not been observed a significant difference of male and female complainants. Right now only few minors seem to address ULD, but there are three main occasions where they ask for help: 1) in case they feel to be treated unfairly, 2) if they have observed IT security problems of data controllers, and 3) if they need help with their homework on some privacy or data protection issue. Several elderly people write their own complaints, some via e-mail, more via mail or they use the phone. In some cases, and this is also true for disabled persons, letters are written by their relatives or by assigned delegates, such as friends, lawyers, or associations specialized on their issues.

Citizens address the DPA through mail, e-mail, phone calls, fax, personal visits. Sometimes requests of individuals are also forwarded by other institutions, e.g. by other DPAs (not being in charge), by the Petition Committee of the Landtag of Schleswig-Holstein, by the Schleswig-Holstein Ombudsperson, by ministries in Schleswig-Holstein. Three kinds of people might face difficulties in addressing the DPA, such as people who don’t know their rights and don’t expect that they have any rights, people who have problems to express the circumstances of a case, people who don’t have the time or nerves to object directly at the data controller’s.

Citizens usually don’t think of requesting prior checking, but have experienced a specific situation where they think that their rights were violated or their privacy was infringed. In these cases they want that the DPA investigates the case and enforces their interests. Often the cases are about denied or ignored access to personal information or other violations of data protection rules (e.g. failure of erasure of personal data from marketing lists, lack of appropriate IT security safeguards, privacy breaches, being asked from authorities or companies to disclose private information, e.g. bank account statements). Some people want to know their rights, but usually they want to get help from the DPA because they didn’t succeed in exercising their rights.

Usually admissible complaints are related to objective breaches of data protection rules. There are very few cases where complaints are not justified. Often this is the case when the general expectation or general data protection principle would not allow the specific data processing, but because of a legal exception to the rule (based on other regulation) the data processing may be lawful (e.g. the disclosure of personal data by registration
authorities to political parties in case the data subjects have not objected; the data processing by the fee collection centre of public-law broadcasting institutions; data retention by telcos (right now not lawful in Germany)).

Usually all justified complaints have to be followed up by correspondence with the respective data controller. This is necessary to clarify the circumstances of a case and to give the data controllers the opportunity to express their view. Mostly a written correspondence is necessary because this has to be part of a court-proof file – this has to be the basis in case of fines or other sanctions. In urgent cases (where evidence might be destroyed), ULD immediately visits the data controller to investigate the case. In these cases the police are asked for their support. So whenever court-proof documentation is necessary, there are inherent delays. If citizens have questions on their rights and don’t request help by ULD for a current situation, usually ULD employees can answer without delay.

About the new data protection framework reform and the collaboration mechanisms

According to the respondent’s view, it is still not clear how the proposed reform might impact the DPA daily activities. It is mentioned that “perhaps the coherence mechanism will require to steadily check the proposed opinions by other DPAs, or there will be additional tasks to translate citizens’ requests that have to be handled by other DPAs in charge into English or other languages”.

With regard to the coordination and collaboration mechanisms already in place, the interviewed reported that there are about weekly, sometimes daily, e-mail communication exchanges among the German DPAs to ask for experiences from other authorities or to discuss legal opinions on specific issues.

Apart from the Art. 29 Working Party on the European level, the annual International Privacy Commissioners’ Conference and other international working groups, there are plenty of coordination activities on the national level, such as, twice a year meetings of the German “Data Protection Commissioners’ Conference”, meetings of the “Düsseldorfer Kreis” for decisions in the private sector, and meetings of more than 20 working groups of the “Data Protection Commissioners’ Conference” and “Düsseldorfer Kreis”.

4.3.13 Greece

About the institution

The Hellenic Data Protection Authority is an independent public authority that was established in 1997. It consist of a President and six members and is assisted by a Secretariat, that consists of three departments, that are the auditors department, the communication and public relations department and the administration and finance department. The mission of the DPA is the protection of privacy and data protection of individuals in Greece. The primary goal is the protection of citizens from the unlawful

180 Main sources of this section is the DPA website
processing of personal data. The DPA offers guidance and support to controllers in their effort to comply with their obligations.

The Greek and English versions of the website are available\(^\text{181}\). All information on legal framework, annual reports (only available in Greek)\(^\text{182}\), decisions, citizens rights, guidelines for data controllers, news and online contact forms.

*About the complaints received:* No information was available

*About the new data protection framework reform and the collaboration mechanisms:* No information was available

4.3.14 Hungary\(^\text{183}\)

*About the institution*

The Parliamentary Commissioner for data protection and freedom of information was the authority responsible for implementation of the data protection law in Hungary. A new Data Protection and Freedom of Information Act, entered into force on January 2012, has established a new Authority replacing the data protection ombudsman. The Authority is an autonomous regulatory organ, headed by a President who is appointed by the President of Hungary on proposal of the Prime Minister. With reference to its competences, the Authority can initiate investigative procedures; can issue a public report or turn the case to courts if the data controllers fails to provide explanations to the alleged breach of data protection law; has the obligation to inform citizens and raise public awareness on data protection issues.

*About the complaints received:* No information was available

*About the new data protection framework reform and the collaboration mechanisms:* No information was available

4.3.15 Ireland\(^\text{184}\)

*About the institution*

The Office of the Data Protection Commissioner in Ireland was established under the 1988 Data Protection Act. The Data Protection Amendment Act, 2003, updated the legislation, implementing the provisions of EU Directive 95/46.

The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Data Protection Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can

\(^{181}\)http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL
\(^{182}\)http://www.dpa.gr/portal/page?_pageid=33,43521&_dad=portal&_schema=PORTAL
\(^{183}\)Main sources of this section is the DPA website
\(^{184}\)Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

The Irish DPA has set up a very user friendly and detailed website. The Annual Reports are available in the dedicated section\textsuperscript{185}. In the respondent’s view, Irish citizens are well informed on the authority’s activities, as the DPA receive extensive media coverage on a wide range of issues concerning data protection and privacy. An online form to contact the DPA is also available in the contact area of the portal. The Irish DPA has not planned to conduct a study on how is citizens’ perception of the DPA and its functions have evolved, and find particular relevant with this respect the findings featured in the Eurobarometer report ‘Attitudes on Data Protection and Electronic Identity in the EU’, which was published in June 2011.

\textit{About the complaints received}

The Irish DPA received over five thousand queries during 2011.\textsuperscript{1,161}complaints were formally investigated even though a multiple of this number of complaints were received which did not proceed to investigation. The vast majority of complaints concluded in 2011 were resolved amicably without the need for a formal decision under Section 10 of the Data Protection Acts or prosecution under the ePrivacy Regulations. In 2011, the Commissioner made a total of 16 formal decisions on whether there had been a contravention of the Data Protection Acts. 12 of these fully upheld the complainant’s assertion that there had been a breach, 1 partially upheld the assertion and 3 rejected the assertion.

In the respondent’s opinion, the DPA is now seeing a definite shift in the nature and type of complaints received by the Office from the traditional complaint related to inappropriate or unfair use of personal data to a clearer technology focus with individuals concerned about the security of their personal data and the uses made of that data by software and technology applications. In 2011 for the first time the number of data breach notifications outstripped the number of complaints opened for investigation.

Email, website and phone are the most common tools to contact the DPA. Two categories of people are addressing the authority, i.e. data subjects (to submit questions about their rights under the acts, about data sharing and potential disclosures, electronic direct marketing) and data controllers (seeking guidance on compliance matters, as well as reporting data breaches).

The DPA do not gather data regarding the age or disabilities of individuals when addressing the DPA. The majority of the complaints received are related to access Rights (48%), while other categories include the electronic direct marketing (22%), data disclosure (10%), the unfair processing of data (5%), or the unfair obtaining of data (4%). In approximately 70% of the cases, the DPA finds a breach of the data protection law. The DPA is committed in acknowledging all queries submitted in writing by citizens

within 3 working days, as well as in keeping individuals informed of progress if a final reply is not issued within 15 working days.

About the new data protection framework reform and the collaboration mechanisms

According to the respondent, the reforms will strengthen the rights of individuals in terms of increased transparency, greater control over processing, data minimisation, specific provisions for processing of children’s personal data, strengthened data access rights/right to object/right to data portability/data deletion (“right to be forgotten”) and strengthened rights of redress.

In terms of co-ordination mechanisms, the Irish Commissioner attends the Article 29 working party meetings and the Office is represented on a number of Article 29 subgroups. The Office participates in groups dealing with cooperation in the fight against crime such as the EUROPOL Joint Supervisory Body, the Customs Joint Supervisory Authority and the EUROJUST Joint Supervisory Body. The Office also conducts informal one to one engagements with individual or multiple DPAs where co-ordination and mutual assistance are provided.

4.3.16 Italy

About the institution

The Italian data protection authority (Garante per la protezione dei dati personali) is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals’ dignity. The DPA was set up in 1997, when the former Data Protection Act came into force. It is a collegiate body including four members, who are elected by Parliament for a seven-year non-renewable term. The authority has an office in Rome with a staff currently numbering about 125 people.

The DPA’s tasks are set forth in the law (the Data Protection Code 196/200), which superseded the Data Protection Act 675/1996 transposing Directive 95/46/EC and implementing the Convention 108 on automatic processing of personal data of the Council of Europe. The DPA competencies include the following: supervising compliance with the provisions protecting private life; handling claims, reports and complaints lodged by citizens; banning or blocking processing operations that are liable to cause serious harm to individuals; checking, also on citizens’ behalf, into the processing operations performed by police and intelligence services; carrying out on-the-spot inspections to also directly access databases; reporting to judicial authorities on serious infringements; raising public awareness of privacy legislation; fostering the adoption of codes of practice for various industry sectors representing the ground for the lawful processing of personal data and subject to publication on the Official Journal (GURI); granting general authorisations to enable the processing of certain data categories (sensitive data) in the private sector.

---

186 Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire.
The DPA draws Parliament’s and the Government’s attention to the need for regulatory measures in the data protection sector and renders mandatory opinions on regulatory instruments and administrative measures drafted by public administrative bodies.

The Annual Report is the occasion not only to inform the Parliament, the Government, the Institutions and the public at large on the activities carried out during the year, but also to offer an overview on the issues considered as the most relevant for the future activity. All the Annual Reports are available on the DPA’s website for the years running from 1997 to 2010. The summaries of the annual reports are also available in English language starting from the year 2000.

The information and outreach policy is an important part of the Italian DPA effort. In this regard, every year the Italian DPA launches initiatives on the occasion of the European data protection day (28th January). Booklets and information leaflets, newsletters, and a daily updated website are produced by the DPA to provide guidance on privacy and data protection issues (e.g. see the booklet "Social Networks: Watch out for Side Effects"). All these activities are meant to foster the knowledge/awareness of the DPA among citizens. At the moment, we do not foresee any study regarding citizens' perceptions towards the Garante.

About the complaints received

As provided for in Section 154 b) of the DP code, one of the main tasks of the authority is “receiving reports and complaints, and taking steps as appropriate with regard to the complaints lodged by other data subjects or the associations representing them”. As reported by statistics available in the annual reports, the handling of complaints represents a huge part of the DPA’s activity.

In 2010, there were 349 decisions on “formal complaints” (“ricorsi”, specifically regulated and time-barred as per sections 145-151 of the DP Code). As was the case for previous years, most of them concerned banks, financial companies and credit reference agencies. The “formal” complaints handled by the DPA over the years only refer to the failure to exercise access/rectification rights. All other cases deal with all possible cases of unauthorized/unlawful/inappropriate processing of personal data. These remedies are called “claims” (“reclami”) and “reports” (“segnalazioni”), and are regulated in sections 142 to 144 of the DP Code.

The yearly statistics published show that the type of such complaints (numbering on average between 3,000 and 4,000 yearly) has been changing to some extent over the years. Cases related to telephony, banking and marketing activities have been steadily present, whilst the frequency of issues concerning credit bureau or the processing of employees’ data or video surveillance has been varying. The number of complaints received by the Garante, having regard to both formal and less formal complaints, is steadily increasing.

---

Regarding the ease of access to the DPA by vulnerable groups of people, the Desk Office plays a special attention towards people less familiar with online services and/or not having an in-depth knowledge of the privacy and data protection aspects. In such cases, the Office, for example, uses a plain-basic language, makes recourse to more traditional methods for communication, such as telephone calls, sends leaflets and other explanatory documents. It can also be remarked that politicians and so-called “VIPS” are often addressing the DPA. Such requests for intervention, even though not the most significant from the statistical point of view, strongly recall the attention of the public opinion on the DPA’s activity due to the wide information provided by Italian media on such cases.

The Italian DPA has a Front Office dedicated to provide prompt replies to citizens, that handles FAQs through telephone, e-mail and standard mail. Some forms (e.g. for requesting access to one’s personal data as held by a data controller, for requesting ad-hoc authorizations, for notifying processing operations) are available via our website (notification, in particular, may only be submitted electronically). More formal requirements (written pleadings, etc.) have to be complied with in order to lodge complaints. As for formal requests, it has to be noted that they can be submitted to the Garante also via certified e-mail (PEC - ‘posta elettronica certificata’).

Citizens are addressing the Italian DPA to lodge claims or reports with regard to the issues mentioned above as well as to get information on the DPA’s activity (decisions already made in given areas, legal requirements, clarification about procedural issues). As for the requests for prior checking, pursuant to section 17 of the DP Code, a specific procedure is envisaged (setting a time constraint of 180 days) and that the payment of fees is also foreseen (according, i.e., to DPA’s Regulations 1 and 2/2007).

In 2010 on 349 formal complaints, 273 were admissible. Among these admissible cases, a breach of data protection rules was found in 51 cases.

The DPA is also strongly committed also to inspection activities. In 2010, around 500 inspections were carried out as a whole. Following the inspections, 55 reports were preferred to judicial authorities and a total amounting to more than 4 million Euro (first semester of 2011 included) was levied via the relevant fines. As for criminal cases, several had to do with the failure to take minimum-level security measures; unlawful data processing operations, the provision of untrue statements and information to the DPA, while non-compliance with orders/measures issued by the DPA was also detected.

Formal complaints (“ricorsi”) are handled according to the procedure and within the timeline set by the DP Code and DPA’s Regulation 2/2007 (60 Days, subject to a prorogation of 40 days for particularly complex cases), without any problem in replying timely to the complainants. Claims (“reclami”), according to Sections 142-143 of the DP Code, may concern any DP issue; timing constraints are 180 days + 90 days for especially complex cases; following which specific measures may be imposed by the DPA. Reports (“segnalazioni”), according to Section 144, may also concern any DP issue; timing constraints are 180 days + 90 days, and measures may be specified by the DPA.
**About the new data protection framework reform and the collaboration mechanisms**

In the respondent’s view, the proposed reform on data protection, extending the obligation to notify data breaches to sectors other than the TLC sector (where such obligation has been introduced by Directive 136/2009), will most probably engender a significant workload for the DPA. In general, the amount of work for the DPA will be increased by the introduction of the obligation to run a data protection impact assessment, and of other new principles, among which we mention: the right to oblivion, the possibility of class actions, the consistency mechanism, the referral to the Court of the DPA, the obligation to appoint a privacy officer.

With reference to the coordination and collaboration mechanisms already in place, the respondent mentioned that the DPA is member of the Article 29 Working Party and participates in European - with particular regard to the work of joint supervisory authorities as per the relevant conventions (Schengen, Europol, Customs Information System) - and international activities (OECD, Council of Europe). The Case Handling Workshops and the BCR Adoption Procedure have also been mentioned in the questionnaire.

### 4.3.17 Latvia

**About the institution**

The Data State Inspectorate (DSI) is a state administration authority and its work is regulated by the Cabinet of Ministers’ Regulations No. 408 of 28 November 2000 “Bylaws of Data State Inspectorate”. The structure of the DSI and the organisation of its work are determined by the Regulations of Data State Inspectorate (the Regulations can be found on the website of DSI – http://www.dvi.gov.lv). DSI commenced its work in 2001, and its functions are determined within the Personal Data Protection Law, the Electronic Documents Law, the Electronic Communications Law and the Law on Information Society Services.

The reports are available on the DSI website, some of them have also been translated in English. The report regarding 2011 will be available in June.

The DSI carried out a public survey at the eve of last year, and one of the questions was regarding how informed are the citizens regarding the work of DSI. 49% of the respondents indicated that they have some information regarding DSI (in 2003 – 23% and 2006 – 30%), so the general information level has been increasing.

**About the complaints received**

Handling citizens complaints is the main assignment of the Latvian DSI. According to the respondent, year by year the number of the complaints received is increasing, as well as they are becoming more sophisticated. In 2011 250 written complaints were received. This does not include the number of cases which had been started in 2010 and continued in 2011. The main topics of the complaints have been: the data transfer to

---

188 Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
debt collecting agencies; the disclosure of information to third parties regarding the public facility services; the disclosure of personal data on internet; the registration of persons at the State Revenue Service as employed in certain companies without them being employed there and without knowing that.

The main data protection breaches were related to data processing without legal ground, excessive collection of data and to exercising the data subject’s access rights. Administrative penalties have been applied in 47 cases.

Citizens address the Inspectorate through phone calls, visits to the office, e-mail and regular paper mail. The delays in replying can occur when some party that is involved in the specific case does not provide the requested information to DSI or the replies provide insufficient information. Then the complainant is informed regarding the data until when the case is prolonged and the reason.

About the new data protection framework reform and the collaboration mechanisms

According to the respondent, both the human resources and financial capacity might represent a major challenge to comply with the duties established by the new framework.

4.3.18 Lithuania

About the institution

The State Data Protection Inspectorate was set up in October 1996 as a supervisory authority for data protection and information systems in the public sector by the Law of the Republic of Lithuania on Legal Protection of Personal Data (LLPPD). In March 1998 its competencies were expanded to the private sector. In January 2001, a new Law entered into force that amended the LLPPD and a re-organisation of the Inspectorate was needed.

About the complaints received: See yearly reports

About the new data protection framework reform and the collaboration mechanisms: No information was available

4.3.19 Luxembourg

About the institution

The DPA was set up on the 1st December 2002. The authority comprises three members who are full time commissioners, and a support group specialised in law and in administrative issues. The DPA mission is directly derived from the provision of

189 Main sources of this section are: the DPA website and the Annual Reports
191 Main sources of this section are: the DPA website, the Annual Reports, Telephone Interview
Directive 95/46. The institution serves as an “expertise centre” (i.e. studying rules and obligations, giving guidance to data protection and advising the government on these issues), as well as a “regulatory centre” (i.e. receiving notifications of data breaches, fulfilling prior checking in the private sector, and handling citizens complaints).

The authority runs a user friendly website, where all relevant information are uploaded, such as legislation, DPA’s decisions, thematic dossiers and other publications. The annual yearly reports are available on the website192. As a consequence of an increased effort in public awareness campaign from 2007 to 2010 (i.e. through newsletters, websites, interviews and press releases), the DPA experienced a significant increase in the requests of information.

With regard to the question whether there are any particular study on how is evolving citizens’ perception towards the institution, in 2006 the authority was thinking about conducting such a research, but for budget reasons the project was not completed. The DPA is relying on the 2 Eurobarometer survey carried out in 2004 and 2007, that offer perspectives also on national situation. It is however felt that nowadays such a type of study would be necessary in order to have a more detailed view on citizens perspectives.

About the complaints received

With reference to the time spent in handling citizens complaints, with respect to the overall activities, in the respondent’s view the percentages are as follows: 1/6 of the DPA’s effort is devoted to handle complaints and investigation; 1/6 to notification of breaches, 2/6 to prior checking; 1/6 to guidance and public awareness campaign, 1/6 to advise the government.

Year by year, the DPA seem to experience a change in the number and types of complaints received. The main sectors involved are video surveillance in public spaces (half of the requests), surveillance at work, new online services, social media and personal digital assistants (i.e. the iPhone), and the sharing of information among public organisations or among them and the private sector.

Citizens pose questions on their rights in a specific case, requesting assistance to access/rectify/delete information, a prior-checking opinion, and reporting violation of data protection rules. Citizens access the DPA mainly through the website or email. This last tool is preferred by the young generation, while elder people usually call by phone, or send a paper mail. The DPA is noticing an evolution as regards the age of complaints, i.e. an increased interest in young generation in data protection, compared for instance to 9 years ago. With reference to the categories of people addressing the DPA, and whether there is an obstacle for some more vulnerable categories, the authority cannot reply since no statistics on this is collected.

According to the respondent view, the DPA usually find breaches of data protection in a half of admissible complaints (40-50%). They are experiencing a slight delay in replying to citizens complaints mainly due to the lack of resources. The need to be “selective” in

order to be effective frequently emerges in handling case by case. Generally speaking, there is a gap between the sensitivity of data protection issues and the awareness about the ways to get efficient remedies.

*About the new data protection framework reform and the collaboration mechanisms*

According to the interviewed person, they are expecting that the proposed reform on data protection will impact on their daily activities, through clearer and simpler rules providing for more opportunities for teenagers and children to have their rights respected. The focus on accountability was also mentioned, e.g. the idea of a mandatory Data protection officer across Europe is welcome – because of responsibility and expertise allocation – but it is pointed out that in small countries it should be an obligation also for small enterprises, with the need of considering not only the size but the activities carried out by the company – whether they collect a huge amount of data), and the Regulation seem still too vague in this respect. Control over online services is another area where a positive impact is expected from the proposed reform.

Coordination and cooperation mechanisms have been already in place since 1995, and would be strengthen through the new rules. These particularly include the joint work carried out in the scope of the Art 29 WP, as well as the Case Handling workshops, and the cooperation with the DPAs in France, Ireland and Germany.

### 4.3.20 Malta

*About the institution*

The Information and Data Protection Commissioner is the supervisory authority committed to protect the individual’s right to privacy and data protection. The Data Protection Act (Cap.440 of the Laws of Malta) transposing Directive 95/46/EC that entered into force in 2003, empowered the Commissioner with the following functions: to create and maintain a public register of all processing operations being notified by Data Controllers; to institute civil legal proceedings in cases where the provisions of the Act have been or are about to be violated; to encourage the drawing up of suitable codes of conduct by the various sectors; to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller; to collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties.

The website of the Commissioner is a user friendly tool that foresees also two online forms, one to lodge a complaints about an alleged data protection law infringement and the other to submit a query.

*About the complaints received:* No information was available

*About the new data protection framework reform and the collaboration mechanisms:* No information was available

---

193 Main sources of this section is the DPA website
4.3.21 Netherlands

About the institution

The Dutch Data Protection Authority was set up in 2001, but a privacy commission in the Netherlands exists since the late 1980s. The institution gathers 80 employees and has an yearly budget of 7 million Euros. It comprises 2 large data protection supervisor departments, i.e. for the public and private sector, a communication department, a legal office and an international office.

Mainly due to budget limitations, the Dutch DPA decided to reduce to a minimum the effort put in handling the individual complaints, that are considered as highly time consuming. To this end, the DPA has a Front Office that is open every morning for 3 hours. Since 2008, however, they realized that it would have been more effective to focus the attention and the limited resources to big cases of data protection breaches. The ultimate goal should be make citizens aware of their rights and able to have them respected by themselves.

All relevant information is available on the website. The Dutch version of the yearly report is available on the website, but only the sort version is available in English. The DPA does not foresee any study on citizens perception on the authority, but the feeling is that citizens are well informed, also through the issue of regular press releases on new investigations, the debates in Parliament on privacy, or advocacy groups campaigns.

About the complaints received

Due to the different focus of the DPA effort, since 2008 the number of individual formal complaints are diminishing, and are now less than 100 in one year. The authority however prefers considering the number of “signals” (i.e. informal contacts to the phone hot-line and the website), that are very much on the rise.

As per the main sector involved, Internet (e.g. spam) and behavioural marketing issues are the hottest topics, but also video surveillance and the ID number are usually subject of individual complaints.

The DPA has no figures on the categories of people addressing the authority, since the signals are anonymous. Citizens usually ask what are their rights in a specific case, how they can send a claim, as well as to request the DPA to enforce their rights. The inventory of signals received can be the basis for an investigation.

About the new data protection framework reform and the collaboration mechanisms

With respect to the potential impact of the proposed reform, according to the respondent’s view, they are still in the process of lobbying and analysing the new framework, but the cooperation and collaboration mechanisms are an interesting point, even if there is still room for improvement.

---

195 Main sources of this section are: the DPA website, Telephone Interview
4.3.22  Poland\textsuperscript{97}

About the institution

The supervisory authority for the protection of personal data in Poland is the Inspector General for Personal Data Protection (Polish abbreviation: GIODO). This one-person authority is appointed by the Sejm of the Republic of Poland (Lower Chamber of the Polish parliament) with the consent of the Senate (Upper Chamber). The term of office of GIODO is 4 years. The same person may hold the office for not more than two terms. The Inspector General is empowered in particular to: supervise the compliance of data processing with the legal provisions on the protection of personal data; consider complaints and issue administrative decisions ordering the adoption of the proper legal state; keep the register of data filing systems and provides information on the registered data files; issue opinions on bills with respect to the protection of personal data; initiate activities to improve the protection of personal data; participate in the work of international organisations and institutions involved in personal data protection issues\textsuperscript{196}. In order to promote the idea of personal data protection GIODO frequently organises training courses on personal data protection, drafts her/his own website, and publishes her/his opinions in trade press.

About the complaints received

Information is available in English only related to the years 2003 and 2004. The number of complaints about the breach of the Act on the Protection of Personal Data submitted in 2004 increased in comparison with the previous years. During this reporting period 1024 complaints were lodged. The number of decisions (i.e. imposing administrative fines) issued in the course of complaint proceedings being conducted in 2004 amounted to 134, compared to 123 in 2003. According to the 2004 report, “analysis of the complaints which were considered in 2004 shows that the fewest reported problems as regards data protection compliance concerned public administration bodies. […] A transfer of personal data accompanying assignments of claims was the most serious problem as regards complaint proceedings last year. This problem was particularly connected with the private sector practice (e.g. telecommunications services providers, banks, public transport ticket inspectors) of transferring personal data of debtors without their consent in connection with the assignment of claims to third parties”\textsuperscript{199}.

According to GIODO 2004 Annual Report, “different actions taken by the Inspector General in the form of orders contained in administrative decisions, submitting the cases to the prosecution bodies or initiating the motions for disciplinary punishment in most cases resulted in non-continuation of illegal data processing. In order to restore the proper legal state and prevent negligence found to happen again in the future computer

\textsuperscript{97}Main sources of this section is the DPA website, the Annual Reports 2003 and 2004
\textsuperscript{96}See the DPA website at \url{http://www.giodo.gov.pl/138/j/en}
systems used so far for personal data processing were improved, additional procedures were introduced and training courses were organised by the controllers"\textsuperscript{200}.

\textit{About the new data protection framework reform and the collaboration mechanisms}

The Polish authority participates in all the international forums in the field of data protection at the international level, such as the Art. 29 WP, the Council of Europe, and, within the former third pillar, the Joints Supervisory Authorities EUROPOL, SCHENGEN and CUSTOMS. International conferences include the DPAs spring conferences, and the Complaints Handling Workshops, and the meetings of the Central and Eastern Europe Data Protection Commissioners.

\textbf{4.3.23 Portugal}\textsuperscript{201}

\textit{About the institution}

The nature, tasks and competences of the Portuguese DPA, the CNPD – Comissão Nacional de Protecção de Dados – are provided by article 21,22 and 23 of Data Protection Act (Law 67/98 of 26 October). The DP Law applies equally to private and public sector, and also to law enforcement data processing. The PT DPA has and exercises all the powers provided by the Data Protection Directive.

According to the respondents, awareness is a never-ending activity and a lot of work can be done in this field. The Portuguese DPA does not have any study or foresee to have it in the near future on the perception towards their activity. However, they do have some indicators – such as the press coverage, the increasing number of notifications and of information requests, the increasing invitations to participate in seminars and conferences – that the perception of the DPAs activity, as well as the awareness on data protection and privacy issues is constantly raising. The activity reports are available in Portuguese in the authority’s website.

\textit{About the complaints received}

The Portuguese DPA investigates all complaints received, and carries out on the spot inspections where necessary. The effort invested is proportionate to the weight of other activities, such as other procedural activities, like authorisations or opinions.

For many years, the number of complaints was quite stable and was low, but in the last couple of years there is an increasing trend. Though the complaints reflect the transversal scope of data protection, one can spot some specific areas which are more subject to complaints. Therefore, the type of complaints have been changing along the years, also following the socio-economic and technological trends. Nowadays, the majority of the complaints received by the DPA concerns spam, video surveillance and monitoring at the workplace, as well as video surveillance, the use of GPS in car fleet, alcohol testing, and so forth.

\textsuperscript{200} Ibid., page 25
\textsuperscript{201} Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
With reference to the categories of citizens addressing the DPA, it is difficult to provide an accurate answer for the respondent, as they do not collect information on age of the complainants. It might however be empirically stated that the complainants are mostly middle age people (30-55) and increasing young people. They do not think that this is related to any vulnerability or exclusion, but has more to do with awareness. If we look back to national and cultural background of the population, the complainants may reflect a generation of people more used to civic intervention and to defend its rights. Concerning minors, the DPA has a dedicated project addressed to young people and schools to raise awareness and to deal with data protection and privacy in a more preventive way.

The DPA receives complaints or information requests by post mail, fax or in specific forms in our website. The DPA also has a Front Office for receiving citizens or data controllers personally and a dedicated phone line called Privacy Line to provide information.

In complaints, people report what they think are violations of data protection rules, describing the concrete case. In information requests, citizens ask about their rights or ask for advice and guidance in a particular case. They usually want to know what they can do in a specific situation, what their rights are and how they can handle things. In line to what was described above on the types of complaints, citizens more often complain about the undue use or indirect collection of their personal data (spam) and of abusive collection or processing of their data (e.g. monitoring at the workplace; video surveillance). Violations concerning access and rectification are irrelevant. There are also complaints about the lack of the right to information or inadequate way of obtaining consent. It can be said that in more around 80 per cent of the cases, the DPA finds out breaches of data protection rules.

The complaints need to be verified in order to collect evidence (also for sanctions purposes), what implies in most of the cases to inspect on the spot. In other easier situations, a letter to the data controller might resolve the problem in a week. Therefore, depending on the nature of the complaint, the time to handle it may vary a lot. In some cases, there are delays, mostly when it comes to inspect thoroughly the security measures adopted in practice.

*About the new data protection framework reform and the collaboration mechanisms*

The Portuguese DPA has already co-operated a couple of times with other DPAs in order to handle complaints related to Internet or spam. The experience shows that in general it takes too long as the requests do not come as a priority.

According to the respondent’s view, the huge change will happen with controllers with the main establishment in other Member State. This will turn the DPA dealing directly with its citizen more as a mailbox with no substantive intervention in the resolution of the complaint. Though this means that the DPA would probably have less work in that respect (or more if the main establishment is in our MS), the impact will be mostly to the data subject, who addresses naturally the DPA of his own country and waits for his rights to be guaranteed by another country.
4.3.24 Romania\textsuperscript{202}

About the institution

The National Supervisory Authority for Data Protection was established as an independent body in 2005. Its tasks are to investigate and prior check the lawfulness of specific data processing performed by controllers, and to impose sanctions in case of breaches of data protection law, and to handle citizens complaints. According to the 2008 yearly report, the DPA carried out investigations according to four main themes, that are data protection in the financial sector, in the medical sector, e-commerce and video surveillance\textsuperscript{203}.

The Authority has established a website, where the yearly reports are available. During the 2008, the Authority carried out specific activities across the country in order to increase people's level of awareness and information regarding personal data protection\textsuperscript{204}.

About the complaints received

In 2008, 550 complaints were received by the DPA. This represent a significant increase in the number of complaints that in the previous year was 51\textsuperscript{205}. Most of the complaints had as a subject the unsolicited commercial messages received, the processing of personal data in the financial sector and the illegal disclosure and processing of data in other circumstances, such as on websites and online services. The DPA is obliged to issue a decision on a specific case by 30 days from the moment the complaint is received.

About the new data protection framework reform and the collaboration mechanisms: No information was available

4.3.25 Slovakia\textsuperscript{206}

About the institution

The Office for Personal Data Protection of the Slovak Republic (hereafter referred as “the Slovak DPA”) is an independent supervisory authority in the area of data protection with the competence overall in the territory of the Slovak Republic.

The Slovak DPA publishes once in two years report on its activities which is published on the Slovak DPA's web page both in Slovak and English language. Last time the Office could not undertake the translation of its report to English due the lack of adequate financial resources which resulted into serious cut-offs of its activities.

\textsuperscript{202} Main sources of this section are: the DPA website and the Annual Reports 2006, 2007, 2008
\textsuperscript{204} Ibid., page 44
\textsuperscript{205} Ibid., page 32
\textsuperscript{206} Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
The Slovak DPA accordingly to allocated budgetary resources orders the public opinion polls monitoring the level of data protection awareness in the Slovak Republic. The citizens are also questioned upon their perception of the national DPA. Apart of that, the Slovak DPA provides interviews and sought information for the relevant mass media and maintains its web page updated responding on the actual data protection issues.

About the complaints received

Among other activities, the Slovak DPA is competent to hear and investigate he complaints of citizens who suspect the breach of their personal data, under the Act on the personal data protection No 428/2002 Coll. available on the Slovak DPA’ web side. The complaints are referred to as the “notifications” lodged by the data subjects and “instigations” lodged by other subjects. Under the Slovak DPA organisation structure there is a department of inspection put in place consisting of sub-department of inspection and analyse and of the inspectors, steered by the chief inspector. The Slovak DPA hears yearly hundreds of complaints and carries out subsequent inspections of controller’s information systems or inspections ex officio based on the annual plan of inspection.

The complaints are of various nature and subject-matter, and they of course reflect the evolution of new technologies. Their number is rather stable and varies between 150-200 each year. The data protection issues of health care provision, travel agencies ‘work, head-hunter’ activities, voluntary and obligatory pension saving funds, e-commerce, loyalty cards were raised, furthermore for example leakage of financial and economic data, legitimate use of biometrical data, illegitimate disclosure of intelligence data, illicit copying and scanning of personal documents, infringements caused by the satellite and cable TV, processing of dead people’s personal data by burial purposes services were dealt on.207

The Slovak DPA is not entitled to evaluate and research the age of complainants or to profile them based on their sex. According to the respondent’s view, any of the vulnerable mentioned groups would be excluded if the mandatory conditions were met and the respective legal representatives chosen if needed.

Each year there are issued up to 200 orders binding for individual controllers to removing the ascertained deficiencies. The Slovak DPA is entitled to directly reply the data subjects in case of all necessary information in place or before making final conclusion to ask any particular subject of public or private sector for cooperation. The time limit for disposing of the complaint should not exceed 60 days. In extraordinary cases, for example by the delay in providing of cooperation by asked subjects and by complexity or volume of case the time period is adjusted and prolonged at most for 6 months. The obligation to provide cooperation is mandatory accompanied with by law defined time limits.

About the new data protection framework reform and the collaboration mechanisms

At this stage, according to the respondent’s view, they are not in the position to anticipate a concrete design of European legislation and its impact on the DPA activities. The hope is that it will affect their activities in a positive way because it should reduce the administrative burden of the companies and the DPA’s administrative burden could be therefore reduced as well. Furthermore, this impact will be conditioned by the clarity of given legislation.

The cooperation mechanism is informally put in place through the participation the Article 29 WP (EU Working Group on data protection). In case of urgency or necessity they also cooperate with partner DPAs.

4.3.26 Slovenia

About the institution

The Information Commissioner is the inspection and offence authority in the area of data protection as provided by the Personal Data Protection Act of Slovenia (PDPA). The Commissioner also performs other tasks as provided by the PDPA, i.e. he issues non-binding opinions and clarifications on specific issues regarding data protection raised by individuals, data controllers, public bodies and international bodies; he is also competent to conduct prior checks regarding biometric measures, transfer of data to third countries and connection of filing systems. In 2010 he was consulted by the legislator and competent authorities regarding 51 Acts and other legal texts. The Commissioner participates in a number of inter-departmental work groups on e-government projects.

The Information Commissioner devotes much effort to awareness rising activities (lectures, conferences, workshops for different public groups, also children). In the course of its awareness rising activities the Commissioner participates at lectures, conferences, workshops for different public groups. Together with the Centre for Safer Internet of Slovenia the Commissioner covers awareness rising activities for children and young people (lectures at schools, publications). It publishes guidelines and brochures, and is very responsive towards the media. The annual reports with all relevant information are available on the Commissioner's website, in English as well.

The result of these activities is that the Commissioner enjoys a very good reputation and public trust, which shows in the results of the representative “Politbarometer” public opinion poll. According to the results the Commissioner comes second in terms of Slovenian citizens’ trust in different institutions. The DPA do not plan any further studies on the matter, however we believe that the strong increase of citizens’ requests each year can be attributed to high visibility of the institution and the reputation the Commissioner enjoys in the public eyes.

Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
About the complaints received

The Information Commissioner’s central activity is inspection supervision where the majority of supervisions are based on citizen’s complaints and requests. In 2010 the Commissioner received 1859 requests for opinions/clarifications from data subjects and replied to them accordingly. It additionally received 628 complaints from data subjects, out of which 477 qualified and were further investigated.

The citizens can contact the DPA by post, via e-mail, fax, with the use of our online form, by telephone. Telephone and e-mail are used most often. In terms of policy issues it is necessary to mention the increasing use of video surveillance. An important issue, raising many concerns, is also the employees’ right to privacy and data protection in the workplace. There is a notable increase of questions regarding (ab)use of social networking sites, spam, viral marketing and such.

Every year an increase of citizen’s requests for the DPA opinion and an increase of the citizen’s complains can be noticed. In 2010 477 complaints have been investigated: 102 for unlawful collection of data, 101 for unlawful transfer of data, 90 for unlawful publication of data, 86 for direct marketing, 85 for denied access of data subject to data, 59 for video surveillance, 47 for data security, and 58 other. 1859 opinions and clarifications regarding different data protection topics have been also issued. 599 inspections were conducted (477 on the basis of citizen complaints): 202 in public sector, 397 in private sector - 179 offence procedures were initiated (45 in public sector, 82 in private sector), of these 36 warnings, 81 admonitions, 35 fines, and 10 payment orders were issued.209

The DPA directly replies to any matter requested by a citizen. The quantity of requests may result in slight delays.

About the new data protection framework reform and the collaboration mechanisms

The Commissioner participates in a number of international bodies: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, WPPJ, International Working Group on Data Protection in Telecommunications, Council of Europe’s Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). The Information Commissioner is appointed as the Vice-President of the Joint Supervisory Body of Europol.

With respect to the impacts of the proposed reform to the DPA daily activities, considering the newly proposed competencies (such as supervision over data breach provisions, cookies provisions, etc.) and the fact that the DPAs’ resources will most likely not be enhanced, the fear is that the workload will impact on their ability to deal with citizen’s claims.

4.3.27 Spain

About the institution

The Spanish DPA was established in 1994 as an independent authority monitoring the observance of the data protection legal framework. The main duties and tasks of the Spanish DPA are defined in the Spanish Data Protection Act (Ley Orgánica 15/1999 de Proteccion de Datos de Caracter Personal, 13 diciembre). Those duties also include the representation of Spain in International bodies related to privacy and data protection.

The Spanish DPA is currently working with a 159 member staff and with an annual operative budget reaching 14 million euro. The DPA has the following structure: the Director and the Consultative Council; the Cabinet, including a Deputy Directorate, the Legal Department and the International Department; the Deputy Directorate; the Deputy Directorate in Register; the General Secretariat. Their activities are based on 4 main pillars, that are (1) awareness raising, (2) advice (including the legal department activities and the help line), (3) enforcement (including register, protection of rights of individuals, audits and inspections, and infringements and sanctions), (4) international cooperation.

The agency makes a continuous effort in improving the level of information with respect to its activities and to provide guidance to all the relevant stakeholders. This effort has been supported by all possible channels. According to the studies on this issue, the perception towards the DPA is globally positive. In a study conducted in 2009-2010 by the Spanish Centre for Sociological research, it was stated that the agency was known more than 50% of the population.

The annual report is a legal obligation for the DPA, since the Data Protection Act make an explicit statement in that sense (art. 37.1.3k of the DP Act). Annual Reports have been published since 2002 and are available in Spanish on the devoted section of the DPA website.

About the complaints received

From the very beginning, complaints handling has been one of the core activities of the Spanish DPA. The structure of the Agency includes a Deputy Directorate of Inspections, mainly dealing with citizens’ complaints and procedures for the protection of personal rights. According to the questionnaire respondend, the number of complaints is consistently growing every year. By means of example, the sum of claims and complaints ranges from about 1000 in 2003 to about 10.000 in 2011, growing by ten times in eight years. The main sectors involved in citizens complaints are: telecommunication, banking and non-banking financial sector, marketing, internet, e-commerce including spam, surveillance (including video-surveillance in public spaces and at work), public administration (including law enforcement) and health.

Citizens can address the institution using several channels, mainly by phone, mail, the website or in person. In 2010, the global amount of requests was 104.826, distributed in

---

210 Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
85,276 phone calls, 15,457 written inquiries, and 4093 visits in person. In addition to that, 13,600 inquiries were received through the website. According to the last figures, the website had three million of visitors along 2011; the same year, more than 135,000 requests from citizens were attended.

Generally speaking, the most usual type of claims are those related to the protection of rights (i.e. access, rectification, erasure, objection), asking for a formal statement of the DPA. According to the last annual report, the information requests received in 2010 included general information, register of files and processing, DP law principles, infringements, scope of the application of the DP law (24%), transfers, citizens rights (28%), inquiries related to specific data files or processing (19%), others (16%).

There are no concrete figures on the specific categories of people addressing the DPA. With respect to more vulnerable groups of people, in the respondent’s view, it is fair to say that the Spanish DPA makes substantial effort in order to avoid lack of attention in respect of their rights. As an example, the DPA is addressing young people through different actions, such as developing an online toolbox to sensitize teenagers. It is also worth to mention that the help lines and the website can be used as a way to contact the DPA for people with special needs. In addition, the Spanish DPA maintains regular contacts with public and private organisations representing the interests of those groups.

The main data protection issues in citizens’ complaints are related to the lack of absence of information related to the processing, or the processing without the consent of the individual, infringements related to the principles of data quality, communication of data to a third party without consent, security of the processing, violation of the duty of secrecy. With reference to the number of admissible complaints where a breach of data protection rules was found, according to the respondent, in 2011 out of 6000 complaints lodged, the DPA issued about 800 decisions related to infringements (that include fines and warning).

Once the complaint is received, the DPA has a limited time (one year) to proceed with the investigation and to decide whether the file should be closed or start an infringement procedures. The DPA has the obligation to send a formal reply to the complainant, as well as to the controller object of the investigation. Delay may occur and are in direct relation to the volume of complaints received.

About the new data protection framework reform and the collaboration mechanisms

In the respondent’s opinion, the Spanish DPA does not expect great changes in their activity with regard to the response to citizens’ claims, due to the fact that in the present legal context the most significant part of the Agency's work is already focused on answering citizens’ questions, claims or complaints.

There will probably be a clear shift in the work related to notification and prior checking activities. Notification of filing systems and processing of data is mandatory in Spain and, according to the draft Regulation, this will not be the case in the future. On the other hand, they expect an increase in the activity related to development of DPIA.
frameworks, previous authorization of some processing activities and possibly codes of conduct.

It is expected that the new European data protection legal framework may have an impact in the activities related to cooperation with other European DPAs in the field of enforcement (i.e. exchange of information, joint measures, joint inspections,...) but also in relation to the work of the European Data Protection Board and in particular of its activity with regard the “consistency mechanism”. It is foreseeable that the coordination mechanisms in place will be extended and enhanced upon approval of the new Regulation. The Spanish DPA is currently a full member of the Article 29 Work Working Party and, as a consequence, participates in all the coordination mechanisms envisaged by the Directive. The same for all those systems and institutions – Europol, Eurodac, Schengen Information System and so on – requesting coordinated supervision. Apart from that, bilateral mechanisms are fully in place. the Spanish DPA is member of the GPEN (Global privacy enforcement network), as well as of the Ibero-American Network of DPAs and of the International Conference of DPAs.

4.3.28 Sweden\textsuperscript{211}

About the institution

The Data Inspection Board is the national Swedish data protection authority and supervise personal data processing in all sectors of society. The Board can issue directives and codes of statutes, inform citizens on their privacy and data protection rights, handles citizens complaints and carries out inspections.

The Swedish version of the annual report is available on the Board website\textsuperscript{212}. Last year, the Data Inspection Board made a study on young people’s attitudes towards privacy. This was a follow up of similar studies in previous years. The reports are available in English on the website\textsuperscript{213}.

About the complaints received

The Board receives complaints from individuals and assess each complaint individually to see if supervision should be initiated or not. In all cases, the individual receives a reply with either information about the rules and the reason for not initiating supervision or that such supervision has been initiated further to the complaint. In this second case, the individual is informed later about the decision in the supervision case. The Data Inspection Board decides autonomously whether supervision should be initiated or not.

The number of complaints for 2011 remains approximately the same as for 2010. In 2010 however, the number of complaints increased quite significantly compared to 2009; from 233 to 332. Recently, most complaints have referred to customer related

\textsuperscript{211} Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
\textsuperscript{213} http://www.datainspektionen.se/in-english/in-focus-youth-and-privacy
issues, the Internet and the employment context. Employment related issues often refer to surveillance issues such as GPS and video-surveillance.

The type of claims varies. A big part of them concerns disclosure of information on the Internet and legal grounds for video surveillance and surveillance of employees. The Board has a specific information service that replies to phone calls and e-mails from citizens and personal data controllers. The number of questions through this service as well as the number of visitors on our website has increased in the last year.

The Board's information service answers questions by e-mail within 2-3 days. Questions that may require more in depth analysis and complaints should be replied to within 2-3 months. Many questions and complaints can be answered on much shorter notice than that.

*About the new data protection framework reform and the collaboration mechanisms*

According to the respondent, the proposal seems to provide stronger means for citizens to demand that a DPA acts on a complaint. It is also stressed that the opportunity for citizens to submit complaints to the DPA is an important principle, but at the same time it is important that there is room for the DPA to make its own priorities.

**4.3.29 The United Kingdom**

*About the institution*

The Information Commissioner’s Office is an independent regulator for the Data Protection Act (transposed version of Directive EC 95/46), the Freedom of Information Act, the Environmental Information Regulations and the ePrivacy Directive. ICO has offices in England, Wales, Scotland and Northern Ireland with approximately 375 staff and an annual budget of £20 million. £15 million is generated by notification fees from data controllers.

The ICO website is a user friendly and complete communication tool. There is a “make a complaint” and a more general “contact us” online forms. The annual reports are available in the devoted section of the website. Since 2003, every year the ICO undertakes an annual track programme, that looks at UK citizen's awareness of data protection issues.

*About the complaints received*

The Information Commissioner must respond to all complaints received. The ICO receives some 30000 complaints per year which are a mixture of freedom of information

---

214 Main sources of this section are: the DPA website, the Annual Reports, the Questionnaire
217 [http://www.ico.gov.uk/about_us/research/information_rights.aspx](http://www.ico.gov.uk/about_us/research/information_rights.aspx)
and data protection complaints. 268 staff are front facing. In general the biggest complaints are regarding subject access requests. In 2010/11 they made up 28% of all data protection complaints.

The table below summarises the main topics/areas mostly covered by the complaints:

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have lost control over the way your information is collected and processed</td>
<td>60%</td>
<td>68%</td>
<td>67%</td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td>Organisations handle the information they collect about you in a fair and proper way</td>
<td>50%</td>
<td>47%</td>
<td>57%</td>
<td>56%</td>
<td>49%</td>
</tr>
<tr>
<td>Existing laws and organisational practices provide sufficient protection of your personal information</td>
<td>39%</td>
<td>40%</td>
<td>44%</td>
<td>46%</td>
<td>34%</td>
</tr>
<tr>
<td>Online companies collect and keep your personal details in a secure way</td>
<td>34%</td>
<td>32%</td>
<td>37%</td>
<td>37%</td>
<td>26%</td>
</tr>
</tbody>
</table>

The Information Commissioner’s office responds directly to data subjects. The ICO does not give a definitive “yes” or “no” regarding a breach but offers a likely or unlikely decision which the data subject could pursue for redress via the courts. The below table shows the number of complaint that are likely/unlikely to be compliant with the data protection law:

<table>
<thead>
<tr>
<th>Compliance likely</th>
<th>3139</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance unlikely</td>
<td>4128</td>
</tr>
</tbody>
</table>

The table does not include complaints about breaches of the Privacy and Electronic Communities Act, that is UK transposed version of Directive 2002/58.

About the new data protection framework reform and the collaboration mechanisms

If the ICO receives a complaint from a UK citizen about an EU data controller established outside the UK it is forwarded to the ICO International Team and then transferred to a specific person at the relevant EU data protection authority. If the complaint is from a foreign citizen about a UK data controller it would come to the International Team first and then be referred to the ICO complaint’s resolution department for direct correspondence with the complainant and copying in the DPA.

4.4 CONCLUSIONS

The European DPAs showed a significant availability to participate and collaborate in this study. Nineteen authorities replied to the questionnaire, in written form or

---

219 Information from questionnaire.
telephone interview. This section summarises the main conclusions of the research, which are divided into four main sections: (1) DPAs structure and competencies, (2) raising awareness activities, (3) handling citizens' complaints, (4) co-ordination and collaboration mechanisms and the expected impact of the proposed new EU data protection legal framework.

4.4.1 DPAs independence and competencies

The first part of the investigation has focused on an assessment of the structure and independence as well as of the competencies of the national DPAs. As outlined in the first part of this report, there is a great variation across Europe with respect to the DPAs’ independence, and this mainly depends on the national legal framework through which the authority was established.

With particular respect to the competencies of the national DPAs, in general, these include the following: to advise the legislator in the process of drafting legislation or regulations relating to the protection of the individual's rights and freedoms with regard to the processing of personal data; to create and maintain a public register of all processing operations notified by data controllers, in order to facilitate access to information for the data subject; to deliver prior-checking opinions before processing operations are carried out; to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller; to institute civil legal proceedings in cases where the provisions of the national data protection act have been or are about to be violated; to encourage the drawing up of suitable codes of conduct by the various sectors and to provide a data protection audit; to raise public awareness on matters of data protection and privacy; to collaborate with supervisory authorities of other countries or at the EU and international level to the extent necessary for the performance of their duties.

European DPAs are often confronted with the problem of limited resources to carry out their tasks. The lack of financial and human resources is often indicated as a major reason preventing the DPA to accomplish its duties.

4.4.2 Awareness-raising activities

Awareness raising is a “never-ending activity”, as stated by one of the interviewed persons. From this study, it became evident that there is a general awareness of the importance of strengthening all communication channels with both the general public and selected stakeholders, e.g., governmental bodies and NGOs operating in this field. These communication channels usually include the maintenance of a user-friendly and frequently updated website, the opening of a front-line desk or dedicated phone lines for citizens who are addressing the DPA, the issuing of a newsletter, press releases and regular interviews with the press, the issue of a yearly report. The yearly report is a legal obligation for the majority of the DPAs interviewed.

According to many respondents, as a consequence of an increased effort in public awareness campaigns in recent years, the DPAs are experiencing a significant increase in requests for information, as well as in the submission of notifications and complaints. However, DPAs usually don’t have or foresee to have in the near future any study on the
perception towards their institution at a national level. They usually rely on the Eurobarometer surveys that are conducted in Europe to have this information.

4.4.3 Handling citizens’ complaints

In all European Union Member States, citizens have the right to request an investigation on the grounds of infringements of the data protection law. National supervisory authorities are entitled to launch a data protection procedure that may involve the correction of inauthentic personal data, the blocking, erasure, deletion or destruction of illegally controlled personal data, a prohibition of the transfer of personal data to third countries, or the obligation to respect the data subject access right.

The study showed that the DPAs are noticing an evolution in the number and type of complaints received. For many years, the number of complaints was quite stable and relatively low, but in the last decade there has been an increase. With regard to the types of complaints, there is an increasing trend in complaints related to data processing in online services. Other sectors mainly include video surveillance in public spaces, surveillance at work, as well as data processing in the public health and financial sectors.

Citizens usually address the DPA to pose questions on their rights in a specific case, to request assistance to access, rectify or delete information, and to report violation of data protection rules. In information requests, citizens ask about their rights or ask for advice and guidance in a particular case. There are also complaints about the lack of the right to information or inadequate way of obtaining consent.

With reference to the categories of citizens addressing the DPA, and to the question whether there are more vulnerable groups of people who are not able to address the authority, it has been difficult for the respondents to provide an accurate answer, since the DPAs do not collect information on sex, age and other personal details from the complainants. No statistics are therefore available on this issue. It might, however, be empirically stated that the complainants are mostly middle age people (30-55) and, in many cases, the number of young people is increasing. Information on the categories of citizens addressing the DPA is, in the respondents’ view, not related to any vulnerability or exclusion, but has more to do with awareness. In some cases, there has been a noticeable increase in interest in young people in data protection, compared to the previous decade.

Citizens increasingly access the DPA mainly through the DPA’s website or e-mail. The DPAs can receive complaints or information requests by post, fax or specific forms on their websites. In many cases, the DPAs also have a front office for receiving citizens or data controllers personally and a dedicated phone line to provide information.

With reference to the ability of the DPA to react on time to citizens’ claims, the time to handle a claim may vary a lot depending on the nature of the complaint. In easy situations, a letter to the data controller might resolve the problem in a week. When the complaint needs to be verified in order to collect evidence, this may require an inspection. Some delays may also occur also when the DPA has to wait for information on data processing from a public institution, a private company or the DPA of another country.
4.4.4  Co-ordination and collaboration mechanisms and the expected impact of the new data protection legal framework

With regard to the question of whether the recently proposed data protection reform is expected to have an impact on the daily activities of the DPA, a few DPAs replied that it is still too early to comment on this, that they are in the lobbying and analysing phase.

Other DPAs replied that some positive impacts may be already noticed, above all in the joint work carried out in the scope of the Art. 29 WP, as well as the case-handling workshops\textsuperscript{220}, and the co-operation with joint supervisory authorities in the field of enforcement (e.g., exchanges of information, joint measures, joint inspections,...), and with DPAs in other countries. Co-ordination and co-operation mechanisms have been already in place since 1995, but they are expected to be strengthened through the new rules, both in the law enforcement field and in relation to the work of the European Data Protection Board and in particular through the “consistency mechanism”. It is foreseeable that the co-ordination mechanisms in place will be extended and enhanced upon approval of the new Regulation.

With regard to the expected positive outcomes of the new data protection reform, in the respondents’ view, the reform will strengthen the rights of individuals in terms of increased transparency, greater control over processing, data minimisation, specific provisions for processing of children’s personal data, strengthened data access rights, the right to object, the right to data portability and the right to data deletion (“right to be forgotten”) and strengthened rights of redress. The obligation for large companies to have a data protection officer (DPO) who will be responsible for dealing with the DPA was also mentioned as a positive outcome of the reform.

\textsuperscript{220} At the Helsinki Spring Conference of the European Data Protection Authorities in 1999 it was agreed to organise twice a year the so called “Complaints Handling Workshops” to discuss approach dealing with complaints. These meetings aim at the exchange of practical experience concerning problems which occurred in the course of complaints proceedings carried out by the national data protection authorities. See GIODO (Inspector General for Personal Data Protection), "The International Complaints Handling Workshop: Evolution & Consolidation", Paper presented at: Spring Conference of European Data Protection Authorities 2004, Rotterdam, 2004. http://www.giodo.gov.pl/data/filemanager_pl/667.pdf
5 References


http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/Year%20Review%202008_en.pdf


Datinspektionen, “Årsredovisning 2011”, Stockholm,


Finn, Rachel, David Wright, Michael Friedewald et al., "Privacy, data protection and ethical issues in new and emerging technologies: Five case studies", Deliverable 2, PRESCIENT Project, 2011.
http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf

http://www.garanteprivacy.it/garante/document?ID=1819554&DOWNLOAD=true


Annexes

A.1 INTERVIEW QUESTIONNAIRE TEMPLATE FOR DATA PROTECTION AUTHORITIES

Dear Madame/Sir,

Thank you for accepting to provide your contribution to this study, which is performed within the scope of the EU funded project PRESCIENT on “Privacy and emerging fields of science and technologies: towards a common framework for privacy and ethical impact assessment”. The study is devoted to analysing to what extent European citizens are accessing their personal information (see http://www.prescient-project.eu/prescient/inhalte/about/work/citizens_perception.php).

The purpose of this questionnaire is to gather contributions from Data Protection Authorities in Europe on citizens’ attitudes towards data protection. We particularly aim to assess to what extent EU citizens have access to their personal information, if they are able to correct it and how DPAs are supporting these claims. We are proposing the following questionnaire to the Data Protection Authorities in all EU Member States. We believe that the collected contributions will be of the utmost importance for our study.

If you agree, the following questions will be posed to you during a short telephone interview. In alternative, you could choose to reply to the questionnaire in a written form. Please let us know, at your earliest convenience, what is your preference by replying to the email that accompanies the questionnaire.

Questionnaire to European Data Protection Authorities

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role
2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?
3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).
4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)
6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

13) Have you already put in place some coordination mechanisms with other DPAs?

Many thanks for your time!

The results of the interviews/questionnaires will be presented during a workshop to be held in May 2012 in Brussels, and will be included into PRESCIENT Deliverable 3 on Citizens perception of privacy, that will be also soon available on the project’s website.

For further information please contact: silvia.venier@cssc.eu

About PRESCIENT

PRESCIENT is a three-year research project funded by the European Commission under its Seventh Framework Programme. The Project is part of the Science in Society activities of DG Research.

PRESCIENT aims to provide an early identification of privacy and ethical issues arising from emerging technologies and their relevance for EC policy. It will contribute to the quality of research in the field of ethics, by distinguishing between privacy and data protection and analysing the ethical, legal and socio-economic conceptualisations of each.
A.2 TELEPHONE INTERVIEWS WITH DATA PROTECTION AUTHORITIES

Luxembourg

Commission Nationale de la protection des données
Telephone interview with Mr. Gérard Lommel, President
Wednesday, 4 April 2012, 4 pm.

Czech Republic

Czech Office for Personal Data Protection
Telephone interview with Vit Zvanovec, Legislation and Foreign Relations Department
Friday, 6 April 2012, 11 am.

The Netherlands

Dutch Data Protection Authority
Telephone interview with Mr. Paul Breitbarth, Senior International Officer
Tuesday, 10 April 2012, 11 am.
A.3 QUESTIONNAIRES RECEIVED FROM EU DATA PROTECTION AUTHORITIES

EDPS

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

The European Data Protection Supervisor (EDPS) is an independent supervisory authority established in 2004 in accordance with Regulation (EC) No 45/2001. It is based in Brussels.

The EDPS is in charge of supervising the processing of personal data by European Institutions and bodies, of advising EU institutions and bodies on all matters relating to the processing of personal data including advice on legislative proposals, and of cooperating with national supervisory authorities in particular as concerns the former 'third pillar' of the EU.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

The handling of complaints constitutes a small part of the EDPS activities. We do not have a precise indicator on how much time is spent on this activity but it is probably less than 5%.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Annual reports of our activities are available on our website, in the section 'publications'. See: http://www.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Publications/AR

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

We are currently undertaking a survey to understand the perception of our stakeholders on our activities. Intermediate - not yet final - results indicate that civil society generally knows our activities (for about 20% it is very well known and for 40 % well known). The results of this survey will help us develop an internal strategy plan. Once finalised, a final report on our strategy plan shall be made public.

Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g. : data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

The number of complaints is stable since 2009. The main issues involved are: breach of data subjects’ rights, such as access to and rectification of data or objection and deletion;
violation of confidentiality; excessive collection of personal data.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

We did not notice any clear pattern in this regard.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

Mainly by email, since 2011 we implemented an internet form which is now often used. Postal correspondence or telephone are rarely used.

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

We only examine complaints which allege a violation(s) of data protection rules. Please see answer in question 5 for details.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

See answer in question 5

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Only in about 5-10% of admissible cases do we find that there is a persistent breach of data protection rules. There is also a number of cases where we find that there is a breach but the data controller corrects it during the inquiry at our request.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens' requests? Are you experiencing any delay in replying?

In simple cases (non admissible cases, information requests) we usually reply within 1-2 weeks. Complex investigations are longer, in some exceptional cases can take even 2-3 years.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens' claims?

For the moment the proposed reform does not affect the rules under which we work, set forth in Regulation (EC) No 45/2001. Our competence and tasks in respect of EU institutions and bodies and claims from individuals against them will therefore remain dealt with similarly as before under the terms of Regulation (EC) No 45/2001.

We will, however, be more involved in the resolution of trans-border claims from individuals against controllers who are not EU institution/bodies when they fall under the consistency mechanism. In such cases the complaint would be dealt with through the European Data Protection Board (EDPB), in which the EDPS will participate as member and for which it will also provide the secretariat. As host of the secretariat, we will have an increased role in facilitating the coordination of supervisory authorities to respond to claims made through the consistency mechanism.

13) Have you already put in place some coordination mechanisms with other DPAs?
Coordination mechanisms are to some extent already in place under Directive 95/46/EC, Article 29 of which set up a working party composed of all the EU data protection authorities (the 'Article 29 Working Party'). The Article 29 Working Party contributes to ensuring consistency in the interpretation of Directive 95/46/EC within the EU.

Furthermore, in the field of ex third pillars system (SIS, VIS, etc), coordinated supervision is done by the EDPS together with national DPAs.

### Belgium

**About you and your institution**

<table>
<thead>
<tr>
<th>1. Please provide us with a brief introduction of your DPAs and an outline of your role</th>
</tr>
</thead>
</table>
| The Belgian Commission for the Protection of Privacy, better known as the Privacy Commission, is an independent authority ensuring the protection of privacy during the processing of personal data. The Commission was established by the Belgian Federal House of Representatives with the Belgian Act of 8 December 1992. It is assisted by a secretariat. As of 1 January 2004, the Commission has been an independent supervisory authority under the auspices of the Belgian House of Representatives. The Commission consists of sixteen members:  
  - a president;  
  - a vice-president;  
  - six permanent members;  
  - eight substitute members.  
The President and Vice-President are the only members occupying a full-time position. The President's position is occupied by a magistrate. The Vice-President’s mother tongue always has to be French when the President is a native speaker of Dutch, and vice versa. Commission members must include at least one legal counsellor, one IT specialist and two individuals with experience in personal data management, in the public and private sector respectively. The sixteen Commission members are all designated for a renewable six-year term. Every one of them, in his or her own way, is an expert in the protection of privacy and personal data management. The Commission’s mission is to ensure that privacy is respected when personal data are processed. Within the Commission, sector committees have been established, which are in charge of supervising a specific sector. |

<table>
<thead>
<tr>
<th>2. With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have a specific office for first-line help dealing with complaints and requests for information made by citizens. There also is a legal department handling complaints requiring more research and requests for opinions coming from the legislator.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, this is a legal obligation for our DPA. The latest edition is available on our website. We are still working on the 2011 edition which is due to be published at the end of June.</td>
</tr>
</tbody>
</table>
4. In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

We try to inform citizens as best we can, mainly through our website and responding to questions we get from the press. No studies are currently planned in this context.

### Categories of citizens addressing the DPA and types of complaints

5. Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

The object of complaints often depends on current events. Last year, for example, Google Street View was launched in Belgium, which caused a peak in the complaints and requests for information addressed to our DPA. Other recurring topics are surveillance cameras, credit registration, press freedom, police and justice, the employer/employee relationship and direct marketing.

6. Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

No.

7. How do people address your institution (e.g. through your website, through phone calls, trough mail)?

We have a contact form on our website, but people can also send us a letter or an e-mail or call our first-line help desk directly.

8. What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Requests for information on their rights, complaints about press articles/photos (related to the right to be forgotten), access to their data in police databases, …

9. What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

Cf. 8.

10. With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

5,9 % - cf. 2011 annual report.

### How is your institution reacting to claims

11. Depending on the complaint, is your institution able to directly reply to citizens' requests? Are you experiencing any delay in replying?

We reply to citizens directly respecting internal deadlines established by service level agreements.

12. How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens' claims?

The data protection reform will give us the power to impose sanctions as opposed to our current power of mediation only. The notification system will probably be abolished, reducing our administrative workload. There may be a higher workload, however,
related to the technical analysis of data breaches, which would have to be notified to the DPA under the proposed data protection regulation. It is then up to the DPA to decide whether the data subjects concerned will also have to be informed.

Moreover, the new regulation introduces the concept of a one-stop shop also for controllers, meaning that data subjects can still address their national authority for problems with a controller, but it will be the DPA of the country where the controller’s main establishment is located that will deal with the complaint at the request of the DPA to which the complaint was submitted.

13. Have you already put in place some coordination mechanisms with other DPAs?

The European Privacy Directive provides for cooperation between DPAs. This cooperation is not official but informal and depends on the willingness of other DPAs to respond to our requests and their workload.

There is one official cooperation mechanism for Binding Corporate Rules, i.e. a cooperation between DPAs of various EU member states for cross-border data transfers by multinationals, which works very well.

Cyprus

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

The Office of the Commissioner for Personal Data Protection is an independent authority in charge for the protection of personal data according to the directive 95/46/EC.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

Our Office gives strong emphasis and priority in examining citizen’s complaints.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Yes, the yearly reports are available on our website in Greek. Summaries of the reports are available on the English part of the website.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

Some citizens are still not aware of the role and the activities of our Institution. We take all the feasible measures to raise the awareness level of the citizen’s according to our budget and stuff limitations but we cannot perform an in-depth study at this point.
Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

The type of complaints that are submitted are not dramatically different each year; we do see however a small increase each year on the number of complaints regarding internet and video-surveillance.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

So far we have not observed any patterns in the categories of people that are filing complaints in general. We do observe, however, that most of the complaints regarding the internet are submitted by younger people.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

People can address our Office through our website, email, telephone, mail and fax.

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Reporting violations of data protection rules and requesting a prior-checking opinion.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

Data misuse and excessive collection of data

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

The percentage of the cases where breaches of data protection rules occur is different each year. The percentage is relatively high, although there are many cases where the complaints deal with issues that do not fall within the responsibilities of our Office or are beyond the scope of the law.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply
to citizens’ requests? Are you experiencing any delay in replying?

According to the general rules of the administrative procedures, our Office, before reaching a conclusion / issuing a decision on a case, has to give the other party the right to express its opinion and comment on the allegations (one month period is given to the other party to reply). In cases where a breach of the law is found, the other party is also given the opportunity to state any reasons why a fine should not be imposed. (another month period is given).

Also, there is a delay in replying in many cases where we need to obtain information from third parties (e.g. ISPs or banks).

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

We are not in a position to estimate this at this stage.

13) Have you already put in place some coordination mechanisms with other DPAs?

We coordinate with other DPAs both on individual cases and on the basis of groups that we participate (e.g. Article 29, Case handling workshop, Contact Network of Spam Authorities (CNSA), International Working Group for Data Protection in Telecommunications).

Denmark

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

The Act on Processing of Personal Data is under the authority of the Danish Data Protection Agency; therefore, it is the agency's duty to ensure that the law is abided by. For more details, please see http://www.datatilsynet.dk/english/

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

20 % (estimated) of the total resources allocated to the Danish DPA

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

You can find the annual report covering 2010 on the website: http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/Aarberetning_2010.pdf
Note that it is not available in English. The annual report covering 2011 is not yet finished.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

Based on the number of telephone calls, emails etc. many citizens – and a growing
number know the DPA – but not all know about our activities. No study planned at this point.

**Categories of citizens addressing the DPA and types of complaints**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)</td>
<td>The number of complaints and questions has doubled from 2007 to 2012. Most dominant sectors regarding complaints: Internet/social networks, credit agencies, telecommunication, financial sector (not only e-banking, but in general), employment/HR.</td>
</tr>
<tr>
<td>6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?</td>
<td>Not the general impression.</td>
</tr>
<tr>
<td>7) How do people address your institution (e.g. through your website, through phone calls, through mail)?</td>
<td>Phone calls and emails mostly.</td>
</tr>
<tr>
<td>8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)</td>
<td>1) Requesting information, 2) asking their rights 3) reporting violations</td>
</tr>
<tr>
<td>9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)</td>
<td>Questions related to the Danish identification number. Questions related to the internet. Deletion and/or rectification.</td>
</tr>
<tr>
<td>10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**How is your institution reacting to claims**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?</td>
<td>1) Yes (after a procedure of asking questions to the controller involved) 2) Yes because of heavy workload.</td>
</tr>
<tr>
<td>12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?</td>
<td>Too early to say!</td>
</tr>
<tr>
<td>13) Have you already put in place some coordination mechanisms with other DPAs?</td>
<td>Handled case by case – taking contact to other DPA’s when needed.</td>
</tr>
</tbody>
</table>
Estonia

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

Our role is to defend the following constitutional rights: right to obtain information about the activity of public agencies; right to inviolability private and family life in the use of personal data; right to access data gathered in regard to oneself.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

We put our efforts into raising awareness in the fields of personal data protection and transparency of public sector.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

You can find our annual reports on our website: http://www.aki.ee/eng/?part=html&id=96

Introductions of the report is translated into English.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

No such study has been carried out recently. As the amount of complaints is increasing, this should mean that the amount of informed citizens should also be increasing.

Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

General statistics is available on the website: http://www.aki.ee/eng/?part=html&id=146. We wouldn’t point to any specific sectors.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

No

7) How do people address your institution (e.g. through your website, through phone calls, trough mail)?

Mainly through e-mail and phone calls (help-line)

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Mainly reporting violations – if there is now violation then we explain the rights of a citizen. We consider denial of access also as a violation.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse;
excessive collection; request of deletion of data)
There are no issues prevailing in our practice.

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?
There is no such statistics.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?
We are able to reply directly to citizens requests.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?
Today it’s too early to comment

13) Have you already put in place some coordination mechanisms with other DPAs?
Yes, regardless of the proposed reform we are carrying out joint inspections with Baltic DPAs

Germany

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role
The Federal Commissioner for Data Protection and Freedom of Information (hereafter: Federal Commissioner) is elected by the German Bundestag. His legal position and his task are laid down in the Federal Data Protection Act (BDSG). According to this Act he is independent in the performance of his duties and only subject to the law. This means for example that in connection with the performance of his duties, the Federal Government is not entitled to give him any instructions with regard to the subject matter. The Federal Commissioner is only subject to the legal supervision of the Federal Government and only with regard to issues relating to service law he is subject to the administrative supervision of the Federal Ministry of the Interior.

His main tasks include the provision of advice to the German Bundestag. The Federal Commissioner impartially provides the German Bundestag with expert knowledge about all developments in the field of data protection and gives recommendations when and by which laws or other measures the German Bundestag should intervene in the development. In addition, the Federal Commissioner advises the Federal Government, all public federal bodies and other bodies (cf. Sect. 26 BDSG). Moreover his tasks include controls (cf. Sections 24, 25 BDSG) and cooperation in matters relating to data protection law at the European and at the international level.
Another main task of the Federal Commissioner is the dealing with requests by petitioners: Anyone who believes his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies of the Federation may appeal to the Federal Commissioner (Sect. 21 BDSG).

The Federal Commissioner has extensive investigative powers. Admittedly, he is not entitled to give instructions. However, when the Federal Commissioner has detected a data breach he has the possibility to report this violation to the law enforcement authorities and to lodge a demand for prosecution. All public federal bodies are obliged to support him and his staff for the performance of their duties. In addition, the Federal Commissioner is responsible for monitoring the direct federal social insurance institutions, telecommunications- and postal service companies and private companies falling within the Security Clearance Check Act.

Public administrative bodies of the Federal States and/or of local governments are monitored by the data protection commissioners of the Federal States. So-called non-public bodies such as companies are subject to the data protection supervisory authorities for the non-public area of the Länder. Their tasks also include the dealing with petitions within their field of responsibility. Also these data protection supervisory authorities have extensive investigative powers.

<table>
<thead>
<tr>
<th>2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2011, among the whole documents the Federal Commissioner received, the amount of petitions was 25%.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every two years the Federal Commissioners publishes an activity report in which he informs the German Bundestag and the public about essential developments in the field of data protection and about the focal points of his tasks. The activity report is ready for download on his website under <a href="http://www.datenschutz.bund.de">www.datenschutz.bund.de</a>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informing the public is one of the Federal Commissioner’s main tasks. In addition to the activity report the public is also informed by active public relations work. We do not know whether there is any study about the Federal Commissioner and his prominence. However, the Institut für Demoskopie Allensbach (Institute of Opinion Research Allensbach) has already published several reports on the subject data protection/data security, for example the report 2009/Nr. 6 “Zu wenig Datenschutz? (&quot;A lack of data protection?&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Categories of citizens addressing the DPA and types of complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in...</td>
</tr>
</tbody>
</table>
The amount of written complaints and requests at the Federal Commissioner's has nearly tripled in the last five years. The number rose from 2,449 requests in 2005 to 6,087 in 2010. As a whole, in this period, about 24,000 citizens appealed to the BfDI in writing. In addition, there are approximately 7,000 telephone calls per year. Admittedly, in 2011 “only” 5,161 citizens appealed in writing to the Federal Commissioner, but last year, his office received more than 9,000 requests for advice per telephone. Most of the requests concern the topics of data protection in the non-public sector, health and social issues, telecommunications- and postal services.

### 6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

As to this matter, there is no statistical information. In many cases, the petitions do not allow to draw any pertinent conclusions.

### 7) How do people address your institution (e.g. through your website, through phone calls, trough mail)?

In response statistics a distinction is only made between petitions in writing and per telephone, no distinction is made between letter, fax and e-mail. In 2011 the Federal Commissioner received for the first time more requests by telephone than in writing (cf. also answer to 5).

### 8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Many requests are relating to the data subjects’ rights to data protection. In addition to general information the petitioners often wish the Federal Commissioner to take action against the data controller.

### 9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

In general the petitioners believe that a data breach has been committed and therefore they appeal to the Federal Commissioner.

### 10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

We do not have any pertinent statistical information.

### How is your institution reacting to claims

#### 11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

Petitions are answered as soon as possible.

#### 12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?
In general there is no additional impact expected, as the Draft Regulation does not deviate too much from the German Data protection legislation. When the respective request would be of a border over spilling interest, the newly developed consistency mechanism could apply (Art.57, 58). But the Art. 29 Working party and the subgroups consults on likewise matters also now most thoroughly, while the procedures are not yet that formalised.

<table>
<thead>
<tr>
<th>13) Have you already put in place some coordination mechanisms with other DPAs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>On national level there are mechanisms of coordination with the federal DPA. On EU level see answer to question no 12, second sentence.</td>
</tr>
</tbody>
</table>

### 1.1.1 Germany – State of Schleswig-Holstein

**About you and your institution**

1. Please provide us with a brief introduction of your DPAs and an outline of your role

**Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein** (ULD, English: Independent Centre for Privacy Protection) is the Data Protection Authority of Schleswig-Holstein, the northernmost Federal State of Germany. Its office with 40 employees is located in Kiel, Germany. The Privacy Commissioner of Schleswig-Holstein, Dr. Thilo Weichert, is head of ULD. ULD is responsible for supervision of both data protection and freedom of information in Schleswig-Holstein.

The basis for the work of ULD is laid down in the State Data Protection Act Schleswig-Holstein (LDSG S-H). This act is one of the most progressive ones worldwide and includes among others provisions on a seal of privacy for IT products and on privacy protection audits for public authorities. In addition to the privacy seal based on German national and regional law, ULD is coordinating the European Privacy Seal Initiative EuroPriSe, which grants privacy seals on the European level in case of a successful evaluation of compliance with European data protection regulation.

Note that LDSG S-H only covers the supervision of the public sector; for the private sector the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) has to be applied. The freedom of information tasks are laid down in the Freedom of Information Act Schleswig-Holstein (Informationszugangsgesetz – IZG). For all relevant laws see https://www.datenschutzzentrum.de/gesetze/

Currently 25 employees are steady staff (civil servants; 24 full-time equivalents). The civil servants have to fulfil the mandatory tasks from LDSG S-H, BDSG and IZG which is the basis for the organization’s work. In addition ULD has the possibility to get funding for research and development projects and to charge for consultance. About 15 employees are working in that area.

Since 1998 ULD has been working on several national and international projects in the field of data security and privacy protection, among others, the EU-funded IST projects

On the departments within ULD:

Dep. 1: service area: organisation of the office, human resources, public relations; education: data protection training courses

Dep. 2: fundamental legal questions on data protection in the public sector, data protection in the areas of government, tax, schools and universities, social matters, medicine etc.; freedom of information

Dep. 3: fundamental technical questions on data protection and privacy technologies, data security, system data protection, technology and media; support of the other departments

Dep. 4: data protection in the private sector, e.g., trade, banking and assurance, associations, address trade and inadmissible advertisement, market and opinion research, video surveillance, employee data protection, internet, geo data, scoring

Dep. 5: data protection in the areas of police and justice

Dep. 6: coordination of studies and projects for privacy by design, e.g., PrimeLife, ABC4Trust, TClouds; cooperation issues; privacy research

Dep. 7 (I): ULD privacy seal; data protection audits

Dep. 7 (II): EuroPriSe – European Privacy Seal; data protection on the international level

Note that Dep. 2, 3, 4 and 5 are active in investigation, consulting, auditing, and enforcement for their respective subject-specific areas.

14) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

ULD does not collect exact statistics on the percentage of working time for different tasks. Further, the percentages vary over time. All citizens’ complaints are taken seriously and are investigated. The effort is dependent on the number of citizens’ complaints because the employees in the supervision part of ULD also regularly schedule general supervision visits in the public and in the private sector that are independent from individual complaints.

15) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Until 2011, ULD provided a yearly report (https://www.datenschutzzentrum.de/material/tb/). In the last revision of the LDSG S-II, a report per every two years is foreseen which will cover the years 2011 and 2012. This report will be presented in the beginning of 2013.
16) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

The citizens living in Schleswig-Holstein are well informed on several of ULD’s activities because of a regular press coverage (newspapers, radio and TV broadcasts, magazines) and information via the ULD website, subscriptions to our mailing lists etc. ULD’s press releases are quite well taken up by the press. Further, journalists from Schleswig-Holstein and beyond ask for comments and statements on privacy and data protection (usually multiple times per day).

This does not mean that all facets of ULD’s work are well known by all citizens. But regarding the possibility to complain, many people address ULD (even if ULD is not responsible).

Moreover, ULD is hosting the Virtual Privacy Office that provides the website/portal of “www.datenschutz.de”. This is regarded as an entry point for German (or German speaking) internet users who are interested in privacy and data protection.

Categories of citizens addressing the DPA and types of complaints

17) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g. : data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

ULD does not collect exact statistics on the percentage of working time for different tasks. But it is safe to state that the amount of complaints has increased.

Many complaints involve data protection on the internet (including advertisement, marketing, e-commerce, personal data put online by others) or video surveillance in public spaces. The number of complaints regarding employee data protection has increased (not only surveillance at work).

Data protection in the social sector has been a hot issue for years, but meanwhile ULD is not in charge of tackling those complaints anymore because this task has been shifted to the Federal Data Protection Commissioner.

Eventually, cases in the medical sector play a bigger role. Quite regular are complaints because of non-shredded medical files in trash bins.

2. Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

In many cases the age of complainants is not known, so no specific assessment can be done.

There has not been observed a significant difference of male and female complainants.

Right now only few minors seem to address ULD, but there are three main occasions where they ask for help: 1) in case they feel to be treated unfairly, 2) if they have observed IT security problems of data controllers, and 3) if they need help with their homework on some privacy or data protection issue.

Several elderly people write their own complaints, some via e-mail, more via mail or they use the phone. But in some cases, and this is also true for disabled persons, letters are written by their relatives or by assigned delegates (friends, lawyers, or associations specialized on their issues).

Some people also ask at first whether ULD’s service will be costful, and only continue their communication after they get the answer that the service will be free.
Three kinds of people might face difficulties:
- People who don’t know their rights and don’t expect that they have any rights (so they won’t find out)
- People who have problems to express the circumstances of a case (they can get help if they discuss their issue with an employee of ULD)
- In cases where the DPA is the second line of defense: people who don’t have the time or nerves to object directly at the data controller’s

3. How do people address your institution (e.g. through your website, through phone calls, through mail)?

Through mail, e-mail, phone calls, fax, personal visits. Sometimes requests of individuals are forwarded by other institutions, e.g. by other DPAs (not being in charge), by the Petition Committee of the Landtag of Schleswig-Holstein, by the Schleswig-Holstein Ombudsperson, by ministries in Schleswig-Holstein.

4. What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Citizens usually don’t think of requesting prior checking, but have experienced a specific situation where they think that their rights were violated or their privacy was infringed. In these cases they want that the DPA investigates the case and enforces their interests. Often the cases are about denied or ignored access to personal information or other violations of data protection rules (e.g. failure of erasure of personal data from marketing lists, lack of appropriate IT security safeguards, privacy breaches, being asked from authorities or companies to disclose private information, e.g. bank account statements). Some people want to know their rights, but usually they want to get help from the DPA because they didn’t succeed in exercising their rights.

5. What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

All of the given examples.

6. With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Usually admissible complaints are related to objective breaches of data protection rules. There are very few cases where complaints are not justified. Often this is the case when the general expectation or general data protection principle would not allow the specific data processing, but because of a legal exception to the rule (based on other regulation) the data processing may be lawful (e.g. the disclosure of personal data by registration authorities to political parties in case the data subjects have not objected; the data processing by the fee collection centre of public-law broadcasting institutions; data retention by telcos (right now not lawful in Germany)).

How is your institution reacting to claims

7. Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

Usually all justified complaints have to be followed up by correspondence with the respective data controller. This is necessary to clarify the circumstances of a case and to give the data controllers the opportunity to express their view. Mostly a written correspondence is necessary because this has to be part of a court-proof file – this has to be the basis in case of fines or other sanctions.
In urgent cases (where evidence might be destroyed), ULD immediately visits the data controller to investigate the case. In these cases the police are asked for their support. So whenever court-proof documentation is necessary, there are inherent delays. If citizens have questions on their rights and don’t request help by ULD for a current situation, usually ULD employees can answer without delay.

8. How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

This is not clear to ULD.
Definitely the daily work will be influenced.
Perhaps the coherence mechanism will require to steadily check the proposed opinions by other DPAs, or there will be additional tasks to translate citizens’ requests that have to be handled by other DPAs in charge into English or other languages?

9. Have you already put in place some coordination mechanisms with other DPAs?

Yes:
Apart from the Art. 29 Working Party on the European level, the annual International Privacy Commissioners’ Conference and international working groups, there are plenty of coordination activities on the national level:
- Twice a year, meetings of the German “Data Protection Commissioners’ Conference” (all chiefs + usually the deputies of the Federal Data Protection Commissioner and the Länder DPAs)
- Twice a year, meetings of the “Düsseldorfer Kreis” for decisions in the private sector
- About twice a year, meetings of more than 20 working groups of the “Data Protection Commissioners’ Conference” and “Düsseldorfer Kreis”
- About weekly, sometimes daily e-mail communication among the German DPAs to ask for experiences from other authorities or to discuss legal opinions on specific issues

Ireland

About you and your institution

1. Please provide us with a brief introduction of your DPAs and an outline of your role

The Office of the Data Protection Commissioner in Ireland was established under the 1988 Data Protection Act. The Data Protection Amendment Act, 2003, updated the legislation, implementing the provisions of EU Directive 95/46. The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers.

The Data Protection Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.
The Irish DPA received over five thousand queries during 2011. 1,161 complaints were formally investigated even though a multiple of this number of complaints were received which did not proceed to investigation.

The vast majority of complaints concluded in 2011 were resolved amicably without the need for a formal decision under Section 10 of the Data Protection Acts or prosecution under the ePrivacy Regulations. In 2011, the Commissioner made a total of 16 formal decisions on whether there had been a contravention of the Data Protection Acts. 12 of these fully upheld the complainant's assertion that there had been a breach, 1 partially upheld the assertion and 3 rejected the assertion.

Annual Report for 2011 – due to be published April 2012.

We are now seeing a definite shift in the nature and type of complaints received by the Office from the traditional complaint related to inappropriate or unfair use of personal data to a clearer technology focus with individuals concerned about the security of their personal data and the uses made of that data by software and technology applications. In 2011 for the first time the number of data breach notifications outstripped the number of complaints opened for investigation.

<p>|</p>
<table>
<thead>
<tr>
<th>Categories of citizens addressing the DPA and types of complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)</td>
</tr>
<tr>
<td>We are now seeing a definite shift in the nature and type of complaints received by the Office from the traditional complaint related to inappropriate or unfair use of personal data to a clearer technology focus with individuals concerned about the security of their personal data and the uses made of that data by software and technology applications. In 2011 for the first time the number of data breach notifications outstripped the number of complaints opened for investigation.</td>
</tr>
<tr>
<td>6. Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?</td>
</tr>
</tbody>
</table>
We cannot provide an answer to this question as we do not gather data regarding the age or disabilities of individuals when engaging with members of the public.

### 7. How do people address your institution (e.g. through your website, through phone calls, through mail)?

Email, website and phone.

### 8. What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

- Data subjects: questions about their rights under the acts, questions about data sharing and potential disclosures, electronic direct marketing.
- Data controllers and data processors: seeking guidance on compliance matters, reporting data breaches.

### 9. What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

- Access Rights (48%)
- Electronic Direct Marketing (22%)
- Disclosure (10%)
- Unfair Processing of Data (5%)
- Unfair Obtaining of Data (4%)

### 10. With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Approximately 70%

### How is your institution reacting to claims

11. Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

We commit in our Customer Charter to acknowledging all queries submitted in writing by citizens within 3 working days, keeping individuals informed of progress if a final reply is not issued within 15 working days.

12. How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

The reforms will strengthen the rights of individuals in terms of increased transparency, greater control over processing, data minimisation, specific provisions for processing of children’s personal data, strengthened data access rights/right to object/right to data portability/data deletion (“right to be forgotten”) and strengthened rights of redress.

13. Have you already put in place some coordination mechanisms with other DPAs?
In terms of co-ordination mechanisms, the Commissioner attends the Article 29 working party meetings and the Office is represented on a number of Article 29 subgroups. The Office participates in groups dealing with cooperation in the fight against crime such as the EUROPOL Joint Supervisory Body, the Customs Joint Supervisory Authority and the EUROJUST Joint Supervisory Body. The Office also conducts informal one to one engagements with individual or multiple DPAs where co-ordination and mutual assistance are provided.

Italy

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

The Italian data protection authority (Garante per la protezione dei dati personali) is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals’ dignity. The DPA was set up in 1997, when the former Data Protection Act came into force. It is a collegiate body including four members, who are elected by Parliament for a seven-year non-renewable term. The authority has an office in Rome with a staff currently numbering about 125 people.


They include the following: supervising compliance with the provisions protecting private life; handling claims, reports and complaints lodged by citizens; banning or blocking processing operations that are liable to cause serious harm to individuals; checking, also on citizens’ behalf, into the processing operations performed by police and intelligence services; carrying out on-the-spot inspections to also access databases directly; reporting to judicial authorities on serious infringements; raising public awareness of privacy legislation; fostering the adoption of codes of practice for various industry sectors representing the ground for the lawful processing of personal data and subject to publication on the Official Journal (GURI); granting general authorisations to enable the processing of certain data categories (sensitive data) in the private sector.

The DPA is member of the Article 29 Working Party (established pursuant to art. 29 of Directive 95/46/EC) and participates in European - with particular regard to the work of joint supervisory authorities as per the relevant conventions (Schengen, Europol, Customs Information System) - and international activities (OECD, Council of Europe).

Moreover, the DPA draws Parliament’s and the Government’s attention to the need for regulatory measures in the data protection sector and renders mandatory opinions on regulatory instruments and administrative measures drafted by public administrative bodies. The Italian DPA submits an annual report to Parliament describing its activities.
2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

As provided for in Section 154 b) of the DP code, one of the main tasks of the authority is “receiving reports and complaints, and taking steps as appropriate with regard to the complaints lodged by other data subjects or the associations representing them”. As you can easily see from statistics available in the annual reports published on the institutional web site, at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1665291, the handling of complaints represents a huge part of the DPA’s activity.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Yes. The Report is the occasion not only to inform the Parliament, the Government, the Institutions and the public at large on the activities carried out during the years, but also to offer an overview on the issues considered as the most relevant for the future activity. All the Annual Reports are available on the DPA’s website (at: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento) for the years running from 1997 to 2010. The summaries of the annual reports are also available in English language starting from the year 2000.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

The information and outreach policy at the Italian DPA is an important part of its activity. In this regard, every year the Italian DPA launches initiatives on the occasion of the European data protection day (28th January). Booklets and information leaflets, newsletters, and a daily updated website are produced by the DPA to provide guidance on privacy and data protection issues (e.g. the booklet “Social Networks: Watch out for Side Effects”). All these activities/deliverables are meant to foster the knowledge/awareness of our activity among citizens. At the moment, we do not foresee any study regarding citizens’ perceptions towards the Garante.

Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

In 2010, there were 349 decisions on formal complaints (which are specifically regulated and time-barred as per sections 145-151 of the DP Code). Like in previous years, most of them concerned banks, financial companies and credit reference agencies. There are other remedies available to citizens before our DPA, which are regulated less stringently than these “formal complaints” (mostly in terms of timing constraints); they are termed “claims” and “reports” and are regulated in sections 142 to 144 of the DP Code. The yearly statistics published with each Annual Report show that the type of such complaints (numbering on average between 3,000 and 4,000 yearly) has been changing to some extent over the years; roughly speaking, cases related to telephony, banking and
marketing activities have been steadily present, whilst the frequency of issues concerning credit bureau or the processing of employees’ data or video surveillance has been varying - even though they still make up for a considerable amount of the cases addressed. The number of complaints received by the Garante, having regard to both formal and less formal complaints, is steadily increasing.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

Regarding the ease of access to the DPA by vulnerable groups of people, the Desk Office plays a special attention towards people less familiar with on line services and/or not having an in-depth knowledge of the privacy and data protection aspects. In such cases, the Office, for example, uses a plain-basic language; makes recourse to more traditional methods for communication, such as telephone calls; sends leaflets and other explanatory documents.

It can also be remarked that politicians and so-called “VIPS” are often addressing the DPA. Such requests for intervention, even though not the most significant from the statistical point of view, strongly recall the attention of the public opinion on the DPA’s activity due to the wide information provided by Italian media on such cases.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

We have a Front Office dedicated to provide prompt replies to citizens, that handles FAQs trough telephone, e-mail and standard mail. Some forms (e.g. for requesting access to one's personal data as held by a data controller, for requesting ad-hoc authorizations, for notifying processing operations) are available via our website (notification, in particular, may only be submitted electronically). More formal requirements (written pleadings, etc.) have to be complied with in order to lodge complaints. As for formal requests, it has to be noted that they can be submitted to the Garante also via certified e-mail (PEC - ‘posta elettronica certificata’).

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

We only have partial statistics on this. The Front Office publishes a breakdown of the emails received yearly, which shows that in general written requests are made to lodge claims or reports with regard to the issues mentioned above [see answer to question 5]) or to get information on the DPA’s activity (decisions already made in given areas, legal requirements, clarification about procedural issues).

As for the requests for prior checking, pursuant to section 17 of the DP Code, we point out that a specific procedure is envisaged (setting a time constraint of 180 days) and that the payment of fees is also foreseen (according, i.a., to DPA’s Regulations 1 and 2/2007).
9) What are the main data protection issues at stake in citizens’ complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

See Reply to question 5). As said, the “formal” complaints (“ricorsi”) handled by the DPA over the years (as regulated by sections 145-151 of the DP Code) only refer to the failure to exercise access/rectification rights. All other cases - addressed via claims/reports - deal with all possible cases of unauthorized/unlawful/inappropriate processing of personal data.

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

In 2010 on 349 formal complaints (“ricorsi”, submitted pursuant to section 145 of the DP Code), 273 were admissible. Among these admissible cases, a breach of data protection rules was found in 51 cases.

We also point out that the DPA is strongly committed to inspection activities. In 2010, around 500 inspections were carried out as a whole. Following the inspections, 55 reports were preferred to judicial authorities and a total amounting to more than 4 million Euro (first semester of 2011 included) was levied via the relevant fines. As for criminal cases, several had to do with the failure to take minimum-level security measures; unlawful data processing operations, the provision of untrue statements and information to the DPA, while non-compliance with orders/measures issued by the DPA was also detected.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

Formal complaints (“ricorsi”) are handled according to the procedure and within the timeline set by the DP Code and DPA’s Regulation 2/2007 (60 Days, subject to a prorogation of 40 days for particularly complex cases), without any problem in replying timely to the complainants.

Claims (“reclami”), according to Sections 142-143 of the DP Code, may concern any DP issue; timing constraints are 180 days + 90 days for especially complex cases; following which specific measures may be imposed by the DPA.

Reports (“segnalazioni”), according to Section 144, may also concern any DP issue; timing constraints are 180 days + 90 days, and measures may be specified by the DPA.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

The proposed reform on data protection (in particular, the proposal for Regulation), extending the obligation to notify data breaches to sectors other than the TLC sector (where such obligation has been introduced by Directive 136/2009), will most probably engender a significant workload for the DPA. In general, the amount of work for the DPA will be increased by the introduction of the obligation to run a data protection impact
assessment, and of other new principles, among which we mention: the right to oblivion, the possibility of class actions, the consistency mechanism, the referral to the Court of the DPA, the obligation to appoint a privacy officer.

13) Have you already put in place some coordination mechanisms with other DPAs?

Article 29 Working Party; Joint Supervisory Bodies Schengen, Customs, Eurodac, Europol; Case Handling Workshops; BCR Adoption Procedure.

Latvia

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role

Data State Inspectorate (hereinafter – DSI) is a state administration authority and the work of DSI is regulated by Cabinet of Ministers Regulations No. 408 of 28 November 2000 “Bylaws of Data State Inspectorate”. The structure of DSI and the organisation of its work are determined by the Regulations of Data State Inspectorate (the Regulations can be found on the website of DSI – http://www.dvi.gov.lv). DSI commenced its work in 2001, and its functions are determined within the Personal Data Protection Law, the Electronic Documents Law, the Electronic Communications Law and the Law on Information Society Services. Please see the annual reports of our inspectorate (some available also in English) for more detailed information.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

It is the main assignment of our office.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Yes, we do. The reports are available on our website. The report regarding 2011 will be available in June.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

We had a public survey at the eve of last year, and one of the questions was regarding how informed are the citizens regarding the work of DSI. 49 % of the respondents indicated that they have some information regarding the work of DSI (in 2003 – 23% and 2006 – 30%), so the general information level has been increasing.

Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g. : data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking
The number of the complaints year by year is increasing, as well as they are becoming more sophisticated. The main topics of the complaints (in 2011 there were 250 written complaints received, not including the number of cases which had been started in 2010 and continued in 2011):

1. data transfer to debt collecting agencies;
2. disclosure of information to third parties regarding the public facility services;
3. disclosure of personal data on internet;
4. registration of persons at the State Revenue Service as employed in certain companies without them being employed there and without knowing that.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

There are no such specific categories.

7) How do people address your institution (e.g. through your website, through phone calls, trough mail)?

Through phone calls, visits to our office, e-mail and regular mail.

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Reporting of possible violations of data protection rules.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

Data processing without legal ground; excessive collection; exercising of data subject’s access rights.

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Administrative penalties have been applied in 47 cases.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

The delays in replying can occur when some party that is involved in the specific case does not provide the requested information to DSI or the replies provide insufficient information. Then the complainant is informed regarding the data until when the case is prolonged and the reason.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?
The capacity (both human resources and financial) can be a major challenge.

13) Have you already put in place some coordination mechanisms with other DPAs?
Yes, we do, both considering some specific cases and ensuring cooperation.

**Portugal**

**About you and your institution**

1) Please provide us with a brief introduction of your DPAs and an outline of your role

CNPD – Comissão Nacional de Protecção de Dados – Portuguese DPA

The nature, tasks and competences of the PT DPA are provided by article 21, 22 and 23 of Data Protection Act (Law 67/98 of 26 October), which is available in our website in French and English versions.
The PT DPA has (and exercises) all the powers provided by the Data Protection Directive.
The DP Law applies equally to private and public sector, and also to law enforcement data processing.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

The PT DPA investigates all complaints received, and carries out on the spot inspections where necessary. The effort invested is proportionate to the weight of other activities, such as other procedural activities, like authorisations or opinions.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

The activity reports are available in Portuguese in our website (www.cnpd.pt ). The report concerning 2011 is still being elaborated, but we expect to release it during April.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

Awareness is a never-ending activity. We do not have any study or foresee to have it in the near future on the perception towards our activity. However, we do have some indicators – such as the press coverage on our activities, the increasing number of notifications and of information requests, the increasing invitations to participate in seminars and conferences – that the perception of the DPAs activity, as well as the awareness on data protection and privacy issues is constantly raising. Nevertheless, as pointed above, there is always work to be done in this field.
### Categories of citizens addressing the DPA and types of complaints

<table>
<thead>
<tr>
<th>5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For many years, the number of complaints was quite stable and was low, but in the last couple of years there is an increasing trend. Though the complaints reflect the transversal scope of data protection, one can spot some specific areas which are more subject to complaints. Therefore, the type of complaints have been changing along the years, also following the socio-economic and technological trends. Nowadays, the majority of the complaints received by the DPA concerns spam, video surveillance and monitoring at the workplace (also video surveillance, the use of GPS in car fleet, alcohol testing, and so forth).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is difficult to provide an accurate answer, as we do not collect information on age of the complainants; but empirically we may say that the complainants are mostly middle age people (30-55) and increasing young people. We do not think that this is related to any vulnerability or exclusion, but has more to do with awareness. If we look back to national and cultural background of the population, the complainants may reflect a generation of people more used to civic intervention and to defend its rights. Concerning minors, the DPA has a dedicated project addressed to young people and schools to raise awareness and to deal with data protection and privacy in a more preventive way. (Likely in the future, they will become complainants).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7) How do people address your institution (e.g. through your website, through phone calls, through mail)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We keep all channels available. The DPA receives complaints or information requests by post mail, fax or in specific forms in our website. The DPA also has a Front Office for receiving citizens or data controllers personally and a dedicated phone line called Privacy Line to provide information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In complaints, people report what they think are violations of data protection rules, describing the concrete case. In information requests, citizens ask about their rights or ask for advice and guidance in a particular case. They usually want to know what they can do in a specific situation, what their rights are and how they can handle things.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In line to what was described above on the types of complaints, citizens more often complain about the undue use or indirect collection of their personal data (spam) and of abusive collection or processing of their data (e.g. monitoring at the workplace; video surveillance). Violations concerning access and rectification are irrelevant. There are</td>
</tr>
</tbody>
</table>
also complaints about the lack of the right to information or inadequate way of obtaining consent.

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

No exact figures available on that, but we would say that in more around 80 per cent of the cases, the DPA finds out breaches of data protection rules.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

As stated above, the complaints need to be verified in order to collect evidence (also for sanctions purposes), what implies in most of the cases to inspect on the spot. In other easier situations, a letter to the data controller might resolve the problem in a week. Therefore, depending on the nature of the complaint, the time to handle it may vary a lot. In some cases, there are delays, mostly when it comes to inspect thoroughly the security measures adopted in practice.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

In what concerns claims on national data controllers, we cannot foresee any relevant changes. The huge change will happen with controllers with the main establishment in other Member State. This will turn the DPA dealing directly with its citizen more as a mailbox with no substantive intervention in the resolution of the complaint. Though this means that the DPA would probably have less work in that respect (or more if the main establishment is in our MS), the impact will be mostly to the data subject, who addresses naturally the DPA of his own country and waits for his rights to be guaranteed by another country. We suppose this would be inexplicable for the data subject, whose personal data is collected and processed in Portugal by a company with which he signed a contract.... but in a no-main establishment for the purpose of the Data Protection Regulation (!).

13) Have you already put in place some coordination mechanisms with other DPAs?

Yes. The Portuguese DPA has already co-operated a couple of times with other DPAs in order to handle complaints related to Internet or spam. The experience shows that in general it takes too long as the requests do not come as a priority.

Slovakia

About you and your institution

1. Please provide us with a brief introduction of your DPAs and an outline of your role

The Office for Personal Data Protection of the Slovak Republic (hereafter referred as “the Slovak DPA”) is an independent supervisory authority in the area of data protection with the competence overall in the territory of the Slovak Republic.
2. **With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?**

Among other activities, the Slovak DPA is competent to hear and investigate complaints of citizens who suspect the breach of their personal data, under the Act on the personal data protection No 428/2002 Coll. available on the Slovak DPA’ web side clicking on English flag the complaints are referred to as the “notifications” lodged by the data subjects and “instigations” lodged by other subjects. Under the Slovak DPA organisation structure there is a department of inspection put in place consisting of sub-department of inspection and analyse and of the inspectors, steered by the chief inspector. The Slovak DPA hears yearly hundreds of complaints and carries out subsequent inspections of controller’s information systems or inspections ex officio based on the annual plan of inspection.

3. **Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).**

The Slovak DPA publishes once in two years report on its activities which is published on the Slovak DPA's web page both in Slovak and English language. Last time the Office could not undertake the translation of its report to English due the lack of adequate financial resources which resulted into serious cut-offs of its activities.

4. **In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?**

The Slovak DPA accordingly to allocated budgetary resources orders the public opinion polls monitoring the level of data protection awareness in the Slovak Republic. The citizens are also questioned upon their perception of the national DPA. Apart of that, the Slovak DPA provides interviews and sought information for the relevant mass media and maintains its web page updated responding on the actual data protection issues.

### Categories of citizens addressing the DPA and types of complaints

5. **Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g. : data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)**

The complaints are of various nature and subject-matter; of course they reflect the evolution of new technologies. Their number is rather stable and varies between 150-200 each year. Besides of the above mentioned topics, the data protection issues of health care provision, travel agencies ‘work, head-hunter’ activities, voluntary and obligatory pension saving funds, e-commerce, loyalty cards were raised, furthermore for example leakage of financial and economic data, legitimate use of biometrical data, illegitimate disclosure of intelligence data, illicit copying and scanning of personal documents, infringements caused by the satellite and cable TV, processing of dead people's personal data by burial purposes services were dealt on.

6. **Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?**

The Slovak DPA is not entitled to evaluate and research the age of complainants or to profile them based on their sex. We do not think that any of the above mentioned groups would be excluded if the mandatory conditions were met and the respective legal representatives chosen if needed.
7. How do people address your institution (e.g. through your website, through phone calls, through mail)?

Through all kind of communication channels. The complaints should be submitted in writing.

8. What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

The notifications upon suspicion of violation of data protection rules combined with collateral requests. The rights of data subjects are directly applicable by the controllers of information systems.

9. What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

All above mentioned. No relevant statistics available

10. With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Each year there are issued up to 200 orders binding for individual controllers to removing the ascertained deficiencies.

How is your institution reacting to claims

11. Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

The Slovak DPA is entitled to directly reply the data subjects in case of all necessary information in place or before making final conclusion to ask any particular subject of public or private sector for cooperation. The time limit for disposing of the complaint should not exceed 60 days. In extraordinary cases, for example by the delay in providing of cooperation by asked subjects and by complexity or volume of case the time period is adjusted and prolonged at most for 6 months. The obligation to provide cooperation is mandatory accompanied with by law defined time limits.

12. How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

At this stage, despite of certain vision we are not in the position to anticipate a concrete design of European legislation and its impact on our activities. We hope that it will affect our activities in a positive way because it should reduce the administrative burden of the companies and our administrative burden could be therefore reduced as well. Furthermore, this impact will be conditioned by the clarity of given legislation.

13. Have you already put in place some coordination mechanisms with other DPAs?

The cooperation mechanism is informally put in place through our participation the Article 29 WP (EU Working Group on data protection). In case of urgency or necessity we cooperate with partner DPAs.
**Slovenia**

**About you and your institution**

1) Please provide us with a brief introduction of your DPAs and an outline of your role

The Information Commissioner is the inspection and offence authority in the area of data protection as provided by the Personal Data Protection Act of Slovenia (PDPA). The Commissioner also performs other tasks as provided by the PDPA: issues non-binding opinions and clarifications on specific issues regarding data protection raised by individuals, data controllers, public bodies and international bodies. The Commissioner is also competent to conduct prior checks regarding biometric measures, transfer of data to third countries and connection of filing systems. In the course of its awareness rising activities the Commissioner participates at lectures, conferences, workshops for different public groups. Together with the Centre for Safer Internet of Slovenia the Commissioner covers awareness rising activities for children and young people (lectures at schools, publications). The Commissioner participates in a number of inter-departmental work groups on e-government projects. The Commissioner was in 2010 consulted by the legislator and competent authorities regarding 51 Acts and other legal texts. The Commissioner also participates in a number of international bodies: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, WPPJ, International Working Group on Data Protection in Telecommunications, Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). The Information Commissioner is appointed as the Vice-President of the Joint Supervisory Body of Europol.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

The Information Commissioner's **central activity** is inspection supervision where the majority of supervisions are based on citizen's complaints and requests. In 2010 the Commissioner received 1859 requests for opinions/clarifications from data subjects and replied to them accordingly. It additionally received 628 complaints from data subjects, out of which 477 qualified and were further investigated.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).

Our annual reports with all relevant information are available on our website, in English as well: https://www.ip-rs.si/index.php?id=308.

The annual report for 2011 is expected to be published in the months to come.

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

As provided under question 1 the Information Commissioner devotes much effort to awareness rising activities (lectures, conferences, workshops for different public groups,
also children). It publishes guidelines and brochures, and is very responsive towards the media. The result of these activities, transparent work and intensive public campaigning is that the Commissioner enjoys a very good reputation and public trust, which shows in the results of the representative “Politharometer” public opinion poll. According to the results the Commissioner comes second in terms of Slovenian citizens’ trust in different institutions.

We do not plan any studies on the matter, however we believe that the strong increase of citizens’ requests each year can be attributed to high visibility of the institution and the reputation the Commissioner enjoys in the public eyes.

Categories of citizens addressing the DPA and types of complaints

<table>
<thead>
<tr>
<th>5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In terms of policy issues it is necessary to mention the increasing use of video surveillance. An important issue, raising many concerns, is also the employees’ right to privacy and data protection in the workplace. There is a notable increase of questions regarding (ab)use of social networking sites, spam, viral marketing and such.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not collect any data on the age of the citizens. Since we most often communicate by e-mail or post, the age is usually not revealed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7) How do people address your institution (e.g. through your website, through phone calls, through mail)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The citizens can contact us by post, via e-mail, fax, with the use of our online form, by telephone. Telephone and e-mail are used most often.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every year we see an increase of citizen’s requests for our opinion and an increase of the citizen’s complaints. In 2010 as mentioned, we investigated 477 complaints: 102 for unlawful collection of data, 101 for unlawful transfer of data, 90 for unlawful publication of data, 86 for direct marketing, 85 for denied access of data subject to data, 59 for video surveillance, 47 for data security, and 58 other. We also issued 1859 opinions and clarifications regarding different data protection topics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>See question 8.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2010 599 inspections were conducted (477 on the basis of citizen complaints): 202 in public sector, 397 in private sector - 179 offence procedures were initiated (45 in public</td>
</tr>
</tbody>
</table>
sector, 82 in private sector), of these 36 warnings, 81 admonitions, 35 fines, and 10 payment orders were issued.

How is your institution reacting to claims

<table>
<thead>
<tr>
<th>11) Depending on the complaint, is your institution able to directly reply to citizens' requests? Are you experiencing any delay in replying?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We directly reply to any matter requested by a citizen. The quantity of requests may result in slight delays.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens' claims?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Considering the newly proposed competencies (such as supervision over data breach provisions, cookies provisions, etc.) and the fact that our resources will most likely not be enhanced, we fear that the workload will impact on our ability to deal with citizen's claims.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13) Have you already put in place some coordination mechanisms with other DPAs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We are active in the Article 29 Working where coordination is being debated.</td>
</tr>
</tbody>
</table>

**Sweden**

*About you and your institution*

<table>
<thead>
<tr>
<th>1) Please provide us with a brief introduction of your DPAs and an outline of your role</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Inspection Board is the national Swedish data protection authority and supervise personal data processing in all sectors of society. Further information about the DIB and our role can be found in English on: <a href="http://www.datainspektionen.se/english/about-us/">http://www.datainspektionen.se/english/about-us/</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens' complaints?</th>
</tr>
</thead>
<tbody>
<tr>
<td>We receive complaints from individuals and assess each complaint individually to see if supervision should be initiated or not. In all cases, the individual receives a reply from us with either information about the rules and our reason for not initiating supervision or that such supervision has been initiated further to the complaint. In this case, the individual is informed later about the decision in the supervision case. The Data Inspection Board decides autonomously whether supervision should be initiated or not.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, we publish an annual report every year. The report is available on our website, but only in Swedish: <a href="http://www2.datainspektionen.se/bt/ladda-ner-a-bestaell?page=shop.product_details&amp;flypage=produktsida.tpl&amp;product_id=146&amp;category_id=10">http://www2.datainspektionen.se/bt/ladda-ner-a-bestaell?page=shop.product_details&amp;flypage=produktsida.tpl&amp;product_id=146&amp;category_id=10</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens' perceptions</th>
</tr>
</thead>
</table>
Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

The number of complaints for 2011 remains approx. the same as for 2010. In 2010 however, the number of complaints increased quite significantly compared to 2009; from 233 to 332. Recently, most complaints have referred to customer related issues, the Internet and the employment context. Employment related issues often refer to surveillance issues such as GPS and videosurveillance.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

No information available.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

We have a specific information service that replies to phone calls and e-mails from citizens and personal data controllers. The number of questions through this service as well as the number of visitors on our website has increased in the last year.

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

The type of claims vary - a big part concerns disclosure of information on the Internet and legal grounds for video surveillance and surveillance of employees.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

See under 8)

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

I have not been able to find any such exact statistics. The number of complaints for 2011 was 312 whereas the number of initiated supervision cases was 247. This is not an exact ratio of complaints that lead to supervision, since some supervision cases may be initiated on our own initiative.

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?
Our information service answers questions by e-mail within 2-3 days. Questions that may require more in depth analysis and complaints should be replied to within 2-3 months. Many questions and complaints can be answered on much shorter notice than that.

**12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?**

The proposal seems to provide stronger means for citizens to demand that a DPA acts on a complaint. The opportunity for citizens to submit complaints to the DPA is of course an important principle, but at the same time there has to be room for the DPA to make its own priorities.

**13) Have you already put in place some coordination mechanisms with other DPAs?**

Not besides the general cooperation mechanisms such as the Article 29 WP, the JSA Schengen etc.

---

**United Kingdom**

**About you and your institution**

**1) Please provide us with a brief introduction of your DPAs and an outline of your role**

The Information Commissioner’s Office is an independent regulator for the Data Protection Act (transposed version of Directive EC 95/46), the Freedom of Information Act, the Environmental Information Regulations and the ePrivacy Directive.

We have offices in England, Wales, Scotland and Northern Ireland with approximately 375 staff and an annual budget of £20 million - £15 million is generated by notification fees from data controllers.

More information can be found here about our organisation. [http://www.ico.gov.uk/about_us/our_organisation.aspx](http://www.ico.gov.uk/about_us/our_organisation.aspx)

**2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?**

The Information Commissioner must respond to all complaints that he receives. We receive some 30000 complaints per year which are a mixture of freedom of information and data protection complaints. 268 staff are front facing.

**3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it not available on the website).**

Here is a link to our last 3 years worth of annual reports [http://www.ico.gov.uk/about_us/performance/annual_reports.aspx](http://www.ico.gov.uk/about_us/performance/annual_reports.aspx)

**4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?**

Every year we undertake an annual track programme which we have done one since 2003. This is a link to last year’s survey [http://www.ico.gov.uk/about_us/research/information_rights.aspx](http://www.ico.gov.uk/about_us/research/information_rights.aspx)

This looks at UK citizen’s awareness of data protection issues
Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g.: data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc.)

See our previous years’ annual reports. In general our biggest complaints are regarding subject access requests. In 2010/11 they made up 28% of all data protection complaints.

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

See our annual track report for this information as above for this information.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

People can telephone, email or write to us. See here for information:
Make a complaint http://www.ico.gov.uk/complaints/data_protection.aspx
Contact us page https://www.ico.gov.uk/Global/contact_us.aspx

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

See our previous years annual reports. In general our biggest complaints are regarding subject access requests. In 2010/11 they made up 28% of all data protection complaints.

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

See our annual track survey. Link to that is here: http://www.ico.gov.uk/about_us/research/information_rights.aspx

As you will see these are the biggest topics that people are concerned about

<table>
<thead>
<tr>
<th>Issue</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have lost control over the way your information is collected and processed</td>
<td>60%</td>
<td>68%</td>
<td>67%</td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td>Organisations handle the information they collect about you in a fair and proper way</td>
<td>50%</td>
<td>47%</td>
<td>57%</td>
<td>56%</td>
<td>49%</td>
</tr>
<tr>
<td>Existing laws and organisational practices provide sufficient protection of your personal information</td>
<td>39%</td>
<td>40%</td>
<td>44%</td>
<td>46%</td>
<td>34%</td>
</tr>
<tr>
<td>Online companies collect and keep your personal details in a secure way</td>
<td>34%</td>
<td>32%</td>
<td>37%</td>
<td>37%</td>
<td>26%</td>
</tr>
</tbody>
</table>

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Please find below information regarding data protection complaints received. This does not include complaints about breaches of the Privacy and Electronic Communities Act (UK transposed version of Directive 2002/58) finished in the financial year 2010/11 with the outcomes requested. The ICO does not give a definitive yes or no regarding a breach but offers a likely or unlikely decision which the data subject could pursue for redress via the courts.
Data Protection complaint casework finished in the financial year 2010/11

<table>
<thead>
<tr>
<th>Compliance likely</th>
<th>Compliance unlikely</th>
</tr>
</thead>
<tbody>
<tr>
<td>3139</td>
<td>4128</td>
</tr>
</tbody>
</table>

How is your institution reacting to claims

11) Depending on the complaint, is your institution able to directly reply to citizens' requests? Are you experiencing any delay in replying?
Yes. The Information Commissioner's office does respond directly to data subjects. We do have backlogs which we have been working hard to get through.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens' claims?
This is something that the ICO is currently working through via a cross office group.

13) Have you already put in place some coordination mechanisms with other DPAs?
Yes. If we receive a complaint from a UK citizen about an EU data controller established outside the UK it is forwarded to the ICO International Team and then transferred to a specific person at the relevant EU data protection authority.

If the complaint is from a foreign citizen about a UK data controller it would come to the International Team first and then be referred to the ICO complaint's resolution department for direct correspondence with the complainant and copying in the DPA.
Dear Madame/Sir,

Thank you for accepting to provide your contribution to this study, which is performed within the scope of the EU funded project PRESCIENT on “Privacy and emerging fields of science and technologies: towards a common framework for privacy and ethical impact assessment”. The study is devoted to analysing to what extent European citizens are accessing their personal information (see http://www.prescient-project.eu/prescient/inhalte/about/work/citizens_perception.php).

The purpose of this questionnaire is to gather contributions from Data Protection Authorities in Europe on citizens’ attitudes towards data protection. We particularly aim to assess to what extent EU citizens have access to their personal information, if they are able to correct it and how DPAs are supporting these claims. We are proposing the following questionnaire to the Data Protection Authorities in all EU Member States. We believe that the collected contributions will be of the utmost importance for our study.

If you agree, the following questions will be posed to you during a short telephone interview. In alternative, you could choose to reply to the questionnaire in a written form. Please let us know, at your earliest convenience, what is your preference by replying to the email that accompanies the questionnaire.

**Questionnaire to European Data Protection Authorities**

**About you and your institution**

1) **Please provide us with a brief introduction of your DPAs and an outline of your role**

The Spanish DPA was established in 1994. We are the independent supervisory authority in Spain that monitors the observance of the data protection legal system.

- We **guarantee and uphold** the fundamental right to the protection of personal data.
- We act **independently** in exercising the functions entrusted to us.

We are currently working with 159 staff members and with an annual operative budget reaching 14 million €. The DPA has the following structure:

- The Director and the Consultative Council
- The Cabinet, including a Deputy Director, the Legal Department and the International Department
- Deputy Directorate on Inspection
- Deputy Directorate on Register
- General Secretariat

Our activity is based on four main pillars:

- Awareness raising
- Advise
  - Legal department.
The main duties and tasks of the Spanish DPA are defined in the Spanish Data Protection Act (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) and implementing legislation. Those duties also include the representation of Spain in international bodies related to privacy and data protection.

In my case, I'm working on the International Department of the Agency with responsibilities related to law enforcement issues and emerging technologies. In that sense, I'm currently a member of a number of coordinated supervision bodies (Europol, Schengen Information System, Customs Information System and Eurodac) as well as a member of some subgroups of the Article 29 Working Party (Technological Subgroup; Borders, Travel and Law Enforcement; Biometrics and eGovernment and Financial data). I'm also a member of the Expert Group on Data Retention as well as of the Expert Group on Internet of things, both set by the European Commission.

2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens’ complaints?

Complaints handling has been, from the very start of its operation, one of the core activities of the Spanish DPA since the Spanish Data Protection Act and the implementing legislation pay special attention to this issue. In that sense, the structure of the Agency includes a Deputy Directorate General of Inspection mainly dealing with citizens’ complaints and procedures for the protection of the person’s rights.

3) Do you foresee a yearly report on your activities? We would appreciate if you could send it to us (if it is not available on the website).

The annual report is a legal obligation for the DPA since the Data Protection Act make an explicit statement in that sense (Art 37.1.k of the DP Act). You can find annual reports (ES) being published since 2002 in http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/index-ides-idphp.php

4) In your opinion are citizens well informed on your activities? Do you foresee a study on how, if this is the case, is evolving citizens’ perceptions towards your institutions?

The Agency makes a continuous effort of improving the level of information with respect to its activities and to provide guidance to all the relevant stakeholders. This effort is done by using all possible channels at our disposal. According to the studies on the issue, the perception towards the Spanish DPA is globally positive. In a study conducted in 2009-2010 by the Spanish Centre for Sociological Research, it was stated that the Agency was known by more than 50% of the
Categories of citizens addressing the DPA and types of complaints

5) Year by year, do you see a difference in the number/type of complaints received? Which sectors are mainly involved? (e.g. : data protection in internet, video-surveillance in public spaces, surveillance at work, e-banking and e-commerce, etc..)

The number of complaints is consistently growing every year. By means of example, the sum of claims and complaints ranges from about 1000 in 2003 to about 10000 in 2011, growing by ten times in eight years. The main sectors are the following:

- Telecommunications (provision of services as well as fraud and creditworthiness issues)
- Banking and non-banking financial sector (including e-baking)
- Marketing
- Internet
- E-commerce (including spam)
- Surveillance (including video surveillance in public spaces and at work)
- Public Administration (including law enforcement)
- Health

6) Do you think there are specific categories of people (age/sex) who are more often addressing a DPA? Do you feel like there are more vulnerable groups of people (elderly, minors, disabled) who are excluded from this process?

There are no concrete figures on the specific categories of people addressing the DPA. With respect to more vulnerable groups of people, it is fair to say that the Spanish DPA makes substantial efforts in order to avoid lack of attention in respect of their rights. By way of example, the DPA is addressing young people through different actions like developing an online toolbox to sensitize young people specifically addressed to the educational community in Spain and Iberoamerica in collaboration with the Spanish Ministry of Education, Culture and Sports. It is worth to mention in the same line the importance of the help-line and the website as ways of contacting the DPA for people with special needs. In addition, the Spanish DPA maintains regular contacts with public and private organisations representing the interests of those groups.

7) How do people address your institution (e.g. through your website, through phone calls, through mail)?

Citizens can address the DPA using several channels, mainly by phone, mail, our website or in person. According to the last figures, our website had three million of visitors along 2011; the same year, more than 135.000 citizens' requests were attended.

In 2010, the global amount of requests was 104.826, distributed in 85.276 phone calls, 15.457 written inquiries and 4093 in person visits. In addition to that, 13.600 inquiries were received – and
answered – through our website.

According to the last annual report, the information requests received in 2010 were distributed according to the following figures:
1. General Information 2,25%
2. Register of files and processing’s 0,34%
3. DP Law principles 5,38%
4. Infringements and penalties 0,14%
5. Scope of application of the DP Law 24,41%
6. Transferences 2,25%
7. Citizen rights 28,81%
8. Questions / inquiries related to specific data files or processing’s 19,56%
9. Others 16,14%

8) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior-checking opinion? Reporting violations of data protection rules?)

Generally speaking, the most usual type of claims are those related to the protection of rights (access, rectification, erasure or objection) asking for a formal statement of the DPA. In that sense, it is worth to mention the growth in the claims related to the right to be forgotten, 160 in 2011

9) What are the main data protection issues at stake in citizens complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)

- Lack or absence of information related to the processing
- Processing without duly consent of the individual
- Infringements related to the principle of data quality (inaccurate, excessive, uncompleted or outdated data)
- Communications of data to a third party without consent
- Security of the processing (including security breaches)
- Violation of the duty of secrecy
- International transfers

10) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

In 2011 were lodged approximately 6000 complaints. The same year, the DPA issued about 800 decisions related to infringements (including fines and warnings).

How is your institution reacting to claims
11) Depending on the complaint, is your institution able to directly reply to citizens’ requests? Are you experiencing any delay in replying?

Once a complaint is received, the DPA has a limited time (one year) to proceed with the investigation and to decide whether the complaint file should be closed or, alternatively, to start an infringement procedure. In both cases the DPA has the obligation to send a formal reply to the complainant as well as to the controller object of the investigation. Delays are in direct relation to the volume of complaints received. Since the resources never grow at the same level as complaints do, some degree of delay is unavoidable in certain cases, also influenced by the complexity of the investigation. Nevertheless, up to now delays are kept to an acceptable level.

12) How do you expect that the proposed reform on data protection will impact on your daily activity, with particular reference to the response to citizens’ claims?

We do not expect great changes in our activity with regard to the response to citizens’ claims due to the fact that in the present legal context the most significant part of the Agency’s work is already focused on answering the questions, claims or complaints that citizens address us.

For instance, the Agency has in place a “Help Line” where citizens may send questions using mail, email, our web page or the telephone. In 2011 we got, and answered, 135,000 questions.

In the field of enforcement of Data Protection Law, citizens already have the possibility to lodge claims or complaints related to infringements of the law. According to our Law, all complaints and claims have to be processed and answered.

In the case of claims, citizens request the intermediation of the Agency to help them to exercise their rights vis-à-vis a controller. Typically, the outcome of these procedures will be a decision of the Agency requesting the controller, if that is the case, to give the data subject access to the personal data that may be processed by the controller or to rectify, cancel or stop processing this data. Where the controller does not follow this request, an infringement procedure will be open.

With regard to complaints, citizens inform the Agency of a potential infringement of the DP Law and if the existence of an infringement is verified the result of the procedure will be an economic sanction.

As said above, in 2011 we got more than 9,000 complaints and claims and the total amount of fines went over 19 million Euro (provisional figures).

There will probably be a clear shift in the work related to notification and prior checking activities. Notification of filing systems and processing of data is mandatory in Spain and, according to the draft Regulation, which will not be the case in the future. But, on the other hand, we expect an increase in the activity related to development of DPIA frameworks, previous authorization of some processing activities and possibly codes of conduct.

It is expected that the new European legal framework may have an impact in the increase of all activities related to cooperation in with other European Data Protection Authorities in the field of enforcement (exchange of information, joint measures, joint inspections,…) but also in relation to the work of the European Data Protection Board and in particular of its activity with regard the “consistency mechanism”.

13) Have you already put in place some coordination mechanisms with other DPAs?

The Spanish DPA is a full member of the Article 29 Working Party and, as a consequence, fully participates in all the coordination mechanisms envisaged by the Directive. The same for all those systems and institutions – Europol, Eurodac, Schengen Information System and so on – requesting coordinated supervision. Apart from that, bilateral mechanisms are fully in place and, thinking on non-EU countries, the Spanish DPA is member of the GPEN (Global privacy enforcement network), as well as of the Iberoamerican network of DPA’s and of the International Conference of DPA’s. It is foreseeable that the coordination mechanisms in place will be extended and enhanced upon approval of the new Regulation.

Many thanks for your time!

The results of the interviews/questionnaires will be presented during a workshop to be held in May 2012 in Brussels, and will be included into PRESCIENT Deliverable 3 on Citizens perception of privacy, that will be also soon available on the project’s website.

For further information please contact: silvia.venier@cssc.eu

About PRESCIENT

PRESCIENT is a three-year research project funded by the European Commission under its Seventh Framework Programme. The Project is part of the Science in Society activities of DG Research.

PRESCIENT aims to provide an early identification of privacy and ethical issues arising from emerging technologies and their relevance for EC policy. It will contribute to the quality of research in the field of ethics, by distinguishing between privacy and data protection and analysing the ethical, legal and socio-economic conceptualisations of each.