
# Fourteenth Annual Report

## of the Article 29 Working Party on Data Protection

*Justice*

This Working Party was set up under Article 29 of Directive 95/46/EC.
It is an independent European advisory body on data protection and privacy.
Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, Belgium, Office No M059 02/013.
Website: http://ec.europa.eu/justice/data-protection/



Luxembourg: Publications Office of the European Union, 2013

ISSN: 1830-6446
ISBN 978-92-79-29769-4
doi: 10.2838/28916

# Fourteenth Report of the Article 29 Working Party on Data Protection

Covering the year 2010

Adopted on 08 December 2011

# Table of Contents

# INTRODUCTION BY THE CHAIRMAN OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY

The technological developments of recent decades have offered consumers many benefits, and have also introduced a whole new online culture and vocabulary, like e-mail, apps and tweets, that consumers have embraced and use in their daily lives. These technological developments and the overwhelming growth of the number of web-based services, have led to a vast increase in the amount of personal data being collected and processed. Together with increasing globalisation, the developments have called for an update of data protection rules.

Throughout 2010, the Working Party continued to focus its work on the review of the legal framework in the European Union and adopted specific opinions related to it, such as on the concept of accountability and on the complex issue of applicable law, as a follow-up to the earlier adopted Joint Contribution to the Consultation of the European Commission of the Article 29 Working Party and the Working Party on Police and Justice of December 2009 (the Future of Privacy report).

The Working Party was very pleased to see that many of the suggestions it made were, to a large extent, incorporated into the European Commission's Communication 'A comprehensive approach on personal data protection in the European Union' of November 2010. The Working Party was also asked by the Commission to provide further advice in 2011, notably on issues such as cooperation between DPAs, notification, sensitive data and consent.

Not only in the European Union, but also in the Council of Europe, the OECD and the United States, data protection and privacy rules are currently under revision. In 2010 in the United States, the Federal Trade Commission issued a preliminary staff report 'Protecting Consumer Privacy in an Era of Rapid Change' and the United States Department of Commerce issued a Green Paper on 'Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework' at the end of the year. This creates an opportunity to strengthen the ties between the European Union and the United States with the aim of providing a high level of data protection across the globe.

Because what in the end is of utmost importance is the effect of the new rules on data protection on citizens, i.e. on data subjects.

More transparency regarding how, by whom and for what reasons data are being collected and processed, is vital. Stressing the importance of transparency may appear politically desirable; however, it can prove to be counterproductive. Nowadays, research claims that each individual person may be registered in 250 to 1 000 different databases, depending on the individual's social and professional activity. It can hardly be expected of data subjects that they keep track of this collection and processing of their data, let alone exercise their rights of access, rectification and deletion of personal data.

Consent remains a cornerstone in the framework of protection of personal data, but relying too heavily on consent as grounds for processing is not always possible, as the conditions for obtaining true informed consent cannot always be met in practice. In today's (online) world, data processing operations are complex, and individuals are faced with many choices. When a privacy policy states that the company 'also shares information with other carefully selected third parties', it remains totally unclear what you are actually consenting to.

One could therefore argue that the fundamental right to data protection cannot be sufficiently guaranteed if the focus lies too much on the actions that need to be taken by individuals themselves to exercise their rights. Therefore the responsibility of controllers to ensure real compliance needs to be strengthened.

Nowadays, there is an increasing need for and interest in data controllers making sure that they take effective measures to deliver real data protection. Maintaining a good reputation, ensuring the trust of citizens and consumers and minimising legal and economic risks are becoming more and more crucial for data controllers. Appointing data protection officers and carrying out data protection impact assessments, which are elements of the so-called accountability principle, can contribute to this.

Following this principle, data controllers would be required to implement the necessary measures to ensure that the material principles and obligations of the law are put into practice when processing personal data. Moreover, they would be required to demonstrate this when requested. In addition, developers of new products and services should also be obliged – at the outset of the development – to think about protecting and securing personal data by means of privacy by design.

In the end, a sound system of data protection can only work if there are checks and balances, and if there is an effective and robust enforcement mechanism in place. Therefore, national data protection authorities need to be equipped with sufficiently strengthened powers to be able to fulfil their tasks properly and in complete independence. In other words, data protection authorities should be enabled to become true enforcement bodies.

Due to the vast increase in cross-border data processing, the need for a uniform application of the legal framework within and throughout the EU, in particular in cases of cross-border supervision and enforcement, is becoming ever more pertinent. The Article 29 Working Party's role in these issues should be strengthened and the Working Party in itself should become more independent.

Finally, to restore the balance between the three main players in the European data protection field, data subjects should be more informed but carry a lighter burden, data controllers should take on their responsibility and be more accountable, and data protection authorities should have more powers to make sure the law is respected, and should be enabled to better cooperate across borders.

**Jacob Kohnstamm**

# Chapter One
# Issues Addressed by the Article 29 Data Protection Working Party[1]

[1] All documents adopted by the Article 29 Data Protection Working Party can be found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

# 1. Issues Addressed by the Article 29 Data Protection Working Party[2]

## 1.1 TRANSFER OF DATA TO THIRD COUNTRIES

### 1.1.1 Passenger Data / PNR

#### Opinion 7/2010 (WP 178) on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries

On 21 September 2010 the European Commission presented its Communication on a global approach to transfers of Passenger Name Record (PNR) data to third countries. The Commission considers that the use of PNR data for law enforcement purposes is growing and is increasingly seen as a mainstream and necessary aspect of law enforcement work.

Therefore, the Commission decided to establish a set of general criteria which should be applied to all future PNR agreements with third countries. The Communication furthermore contains an analysis of the current use of PNR data and lists the third countries with which the Commission plans to conclude agreements in the coming years.

As more and more countries are requesting PNR data, the number of agreements is likely to rise as well. The Commission has decided it is therefore desirable to define a framework which will be applicable to all future PNR agreements, in order to avoid legal uncertainty for both airlines and Member States, as well as unnecessary administrative burdens caused by the need to comply with different sets of rules for the various third countries. The Article 29 Working Party welcomes the global approach taken by the Commission to deal with requests at an EU level and to ensure strong data protection standards in full respect of fundamental rights.

The Working Party wishes to stress that the exchange of PNR data should not be considered in isolation. Therefore, the global approach should be extended to third country requests for all passenger data, including API data, watch-list matching and other pre-screening activities. This means that the Commission should also decide, upon receipt of a request for passenger data, whether the data, and also which kind of data, for example API data, would be sufficient, and conclude an agreement to that effect.

As far as PNR data are concerned, the Working Party closely followed the negotiations that led to PNR agreements with the US, Canada and Australia, and it has issued a number of opinions identifying privacy issues related to these PNR systems. Up to now, many of the objections raised by the Working Party have not been addressed. The current Communication, however, is a step in the right direction, although several concerns remain.

CONCLUSION

Overall, the Working Party is satisfied with the fact that the European Commission is showing clear understanding of the need to pay more attention to data protection in future PNR agreements and is willing to conclude binding agreements to ensure legal certainty and equal treatment. The Communication presented on 21 September 2010 is a step in the right direction. However, the usefulness of large-scale profiling on the basis of passengers' data must be questioned thoroughly, based on scientific elements and recent studies.

The Working Party emphasises once again the need for a global approach to all passenger data and not only PNR data. Coherence is needed in light of current developments, including the review of the EU data protection legal framework and the proposed negotiations with the US on a general data protection agreement.

The Working Party emphasises that the general standards and criteria included in the Communication should be seen as the minimum level of data protection to be achieved in future PNR agreements. However, on several points the standards could and should be further developed.

The Working Party therefore urges the Commission, the European Parliament and the Council to take this opinion into account when discussing negotiating mandates for, and draft versions of, future PNR agreements, and to keep it informed about the follow-up. Naturally, the Working Party is available to work with any of the EU institutions when clarification or elaboration of its position is required.

[2] All documents adopted by the Article 29 Data Protection Working Party can be found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

Finally, the Working Party would like to request once more to be consulted or asked for advice on the data protection elements of any future agreement, especially given its role as an official EU data protection advisory body and the fact that the members of the Working Party are the national supervisory authorities for the carriers that will be obliged to comply with any future agreements. It would also like to be regularly updated on the state of play during the negotiations on these future agreements.

## 1.1.2. Adequacy

### Opinion 6/2010 (WP 177) on the level of protection of personal data in the Eastern Republic of Uruguay

On 20 October 2008 the Mission of the Eastern Republic of Uruguay (hereafter 'Uruguay') to the European Union sent a letter to the European Commission to transmit the official request of the Uruguayan Government to initiate the procedure to declare that Uruguay provides an adequate level of protection with regard to transfers of personal data from the EU/EEA, pursuant to Article 25(6) of Directive 95/46/EC on the protection of personal data ('the Directive').

In order to assess whether Uruguay provides an adequate level of protection, the Commission requested a report from the Centre de Recherche Informatique et Droit (CRID) of the University of Namur. This lengthy report analysed the degree to which the Uruguayan legal system complies with requirements in terms of substantive legislation and the implementation of mechanisms to apply regulations protecting personal data, as set out in the working paper 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive', approved by the Working Party created in relation to Article 29 of the Directive on 24 July 1998 (document WP12). The Uruguayan authorities, via the Unit for the Regulation and Control of Personal Data (URCDP), by agreement of the Executive Council of the URCDP on 11 February 2010, made comments in answer to the issues raised in this report.

The report, as well as the comments of the Uruguayan authorities, were assessed by a subgroup set up specifically for this purpose within the Article 29 Working Party, at the request of which the Chairman of the Working Party notified the Uruguayan authorities of those issues which required further clarification.

The Uruguayan authorities, by means of the URCDP, sent the Article 29 Working Party a lengthy report, approved by agreement of its Executive Council of 23 June 2010, giving its responses to the questions raised in this letter. They also provided a range of documentation on the situation regarding data protection in the country, including this body's annual report for 2009 and its activity report up to 31 May 2010, various resolutions passed by its Executive Council, and relevant legal resolutions on the issue of personal data protection.

This report was redistributed in September 2010 to the members of the subgroup, which analysed it focusing particularly on the issues raised in the letter sent by the Chairman of the Working Party to the Uruguayan authorities. Having analysed the additional information, the subgroup submitted its draft opinion to the Working Party.

On 12 October 2010, the Working Party delivered its opinion that the Eastern Republic of Uruguay ensures an adequate level of protection within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

The Working Party also highlights the fact that, following the decision taken by the Commission, it will closely follow the evolution of data protection in Uruguay and the way in which the Data Protection Authority (URCDP) applies the principles of data protection referred to in document WP12 and in its opinion.

### 1.1.3. Standard Contractual Clauses

#### FAQs (WP 176) in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC

On 5 February 2010, the European Commission adopted a decision updating the standard contractual clauses for the transfer of personal data to processors established in non-EU countries that do not ensure an adequate level of data protection (contractual clauses 'controller to processor').

The new Decision 2010/87/EU regulates the transfers of data between EEA-based controllers and non-EEA-based processors and lists the conditions for sub-processing of data between the non-EEA-based processor and non-EEA-based sub-processors.

On 12 July 2010 the Working Party adopted a document consisting of frequently asked questions (FAQs) addressing issues raised by the entry into force of these updated contractual clauses on 15 May 2010. This document reflects the harmonised position of the European data protection authorities.

The FAQs are not exhaustive and can be updated as required.

## 1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

#### Opinion 2/2010 (WP 171) on online behavioural advertising

Behavioural advertising involves tracking internet users while they are browsing the web and building up profiles over the course of time, which are then used to offer advertising that corresponds to their areas of interest. The opinion specifies the legal framework that applies to those wishing to use behavioural advertising.

The Working Party stressed in particular that advertising network providers are subject to article 5, paragraph 3 of the Directive on Privacy and Electronic Communications, which prohibits placing cookies or similar devices on the user's terminal equipment or accessing information via these devices, except with the informed consent of the user.

It therefore requires advertising network providers to put in place prior "opt-in" mechanisms, which require positive action on the part of the person affected, allowing them to indicate their acceptance that cookies or similar devices may be placed on their equipment and that their behaviour on the internet will be tracked for the purposes of sending personalised advertising.

The Working Party considers that by accepting cookies on one instance, users also provide their acceptance for subsequent readings of the cookie, and consequently, for their navigation on the internet to be tracked.

Since behavioural advertising rests on the use of identifiers that allow the creation of extremely detailed user profiles, which will usually be considered data of a personal nature, Directive 95/46/EC also applies. The Working Party explains how online advertising network providers must adhere to the obligations that this Directive imposes, notably on the subject of the rights concerning access, rectification, erasure, storage, etc.

The opinion analyses and specifies the obligations that are provided for by the applicable legal framework. It does not, however, prescribe the manner in which these obligations must be fulfilled, on the technical level. However, the Working Party invites the professionals affected to engage in dialogue with it in different areas, in order to suggest technical solutions and other ways of adhering to the framework described in the opinion, within the shortest possible timeframe.

## 1.3. ENFORCEMENT

### Report 1/2010 (WP 172) on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations from national traffic data retention legislation on the legal basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive

- This supervisory activity carried out by the Article 29 Working Party to ensure the application of EU legislation was chosen with a view to monitoring respect for the provisions introduced by Directive 2006/24/EC, taking into account the recommendations and concerns expressed by the Working Party in its previous opinions on the topic.
- The application of the Directive on the storage of data by providers of electronic communication services and internet service providers (ISPs) is, by its very nature, associated with a higher level of risk, which makes appropriate technical and organisational security measures necessary.
- On the basis of a questionnaire and spot checks, which the main operators and national ISPs underwent in order to cover a significant part of the market, the activity revealed a patchwork of application measures, notably relating to the security measures being used.
- The Article 29 Working Party is concerned that the Directive does not appear to have been applied uniformly on the national level. It seems, in particular, that it has been interpreted by the Member States as leaving to their discretion the limits of its field of application; indeed, does the Directive intend to allow the general obligation of erasing traffic data as soon as they are no longer necessary for the transmission of a communication to be waived, or alternatively does it intend to make obligatory the storage of all the data that the suppliers are already authorised to keep under article 6, paragraph 2 of Directive 2002/58? The Article 29 Working Party supports this second interpretation, which has also been accepted in the ECJ's recent ruling in the Ireland v Commission case (C 301/06).

The group has made the following recommendations:

- Categories of data to be stored: the list of traffic data that is subject to compulsory storage must considered as exhaustive. As a consequence, no additional data storage obligations can be imposed on providers under the Data Retention Directive.
- Retention periods: in order to achieve greater harmonisation, the maximum data retention period should be reduced and a single, shorter period should be fixed which would be applicable to all EU providers, as was indicated by the Article 29 Working Party in its opinion WP113. Taking a wider perspective, the general security of traffic data itself needs to be reconsidered by the Commission.

Technical and organisational security measures: other specific measures (such as the implementation of a solid authentication system and the establishment of a detailed access log) have been outlined, and a suggested standard for transferring data to law enforcement authorities has been formulated in order to ensure quick and more reliable transfers, allowing the collection of statistical information, as well as responsible access to data. In this context, the notion of "serious breach" seems to need clarification at the level of Member States and the list of entities authorised to gain access to these data must be communicated to all parties concerned.

## 1.4. RFID

### Opinion 5/2010 (WP 175) on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

The Working Party is analysing the industry proposal which would involve implementing the Commission's recommendation to analyse the impact of RFID techniques on privacy.

The Working Party has reservations about one part of the suggestion:

- The classification of applications. Some applications, for which the industry presumes personal data is not processed, are wrongly classified and process personal data on the basis of the unique identifier contained in the RFID tag. For these applications, an impact analysis must be conducted.
- The absence of any consultation of the parties concerned during the process.
- The case of processing individual data, for which more precise recommendations must be made.

The Working Party is convinced that the companies can suggest an improved framework on the basis of observations formulated in this opinion and is working towards implementing all relevant methods in order to continue improving the framework proposal and to achieve its rapid approval.

## 1.5. PERSONAL DATA

### Opinion 3/2010 (WP 173) on the principle of accountability

The opinion describes the benefits for data protection that can come about as a result of concrete measures and practices within companies and administrations. In the absence of any real integration in the common values and practices of an organisation and without an explicit distribution of responsibilities, respect for these principles and obligations risks being compromised and incidents relating to the protection of data are likely to continue.

In order to promote effective data protection, the European regulatory framework must rely on complementary tools. In this respect, the opinion formulates a concrete proposal, with a view to establishing a principle of responsibility, requiring those responsible for processing data to put in place appropriate and effective measures to guarantee respect for the principles and obligations defined in the Directive and to be able to prove these to the monitoring authorities on request. This will contribute to making the data protection a reality and will help the relevant authorities in conducting their work of supervision and implementation.

The opinion also contains proposals that aim to guarantee that the principle of responsibility offers the required legal security, while allowing those involved in protection some room for manoeuvre (for example, by allowing them to determine concrete measures to be put in place according to the risks linked to the kind of processing and the types of data being processed). It then examines the impact that such a principle could have on other areas, including international data transfers, notification requirements and sanctions and, finally, it touches upon the development of certification programmes or labels.

### Opinion 8/2010 (WP 179) on applicable law

This opinion clarifies the scope of application of Article 4 of Directive 95/46/EC, which determines which national data protection law(s) adopted pursuant to the Directive are applicable to the processing of personal data. The opinion also highlights some areas for possible further improvement.

Determining the application of EU law to the processing of personal data serves to clarify the scope of EU data protection law both in the EU/EEA and in a wider international context. A clear understanding of applicable law will help to ensure both legal certainty for controllers and a clear framework for individuals and other stakeholders. Furthermore, a correct understanding of the applicable law provisions should ensure that no lacunae or loopholes are found in the high level of protection of personal data provided by Directive 95/46/EC.

The opinion also provides guidance and examples with regard to: the other provisions of Article 4; the security requirements stemming from the law applicable pursuant to Article 17(3); the possibility for data protection authorities to use their powers to verify and intervene in a processing operation that is taking place on their territory even if the law applicable is the law of another Member State (Article 28(6)).

The opinion also suggests that the wording used in the Directive and the consistency between the different parts of Article 4 would benefit from further clarification as a part of the revision of the general data protection framework.

From this perspective, simplifying the rules for determining applicable law would consist of a shift back to the country of origin principle: all establishments of a controller within the EU would then apply the same law – that of the main establishment – regardless of the territory in which they are located. However, this could only be acceptable if a comprehensive harmonisation of national legislation is reached, including harmonisation of security obligations.

Additional criteria could apply when the controller is established outside the EU, with a view to ensuring that a sufficient connection exists with the EU territory, while avoiding the EU territory being used to conduct illegal data processing activities by controllers established in third countries. In this regard, the following criteria may be developed: the targeting of individuals, resulting in the application of EU data protection law when the activity involving the processing of personal data is targeted at individuals in the EU; and the application of the equipment criterion in a residual and limited form, which would address borderline cases (data on non-EU data subjects, controllers having no link with the EU) where there is relevant data-processing infrastructure in the EU.

CONCLUSIONS

This opinion seeks to clarify the scope of application of Directive 95/46/EC, and in particular Article 4 of the Directive. However, it also highlights some areas for possible further improvement.

## 1.6. CODE OF CONDUCT

### Opinion 4/2010 (WP 174) on the European Code of Conduct of FEDMA for the use of personal data in direct marketing

Article 27, paragraph 3 of the Directive deals with Community codes of conduct in the following terms: Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

In order to facilitate the application of this provision, the Working Party adopted, in September 1998, a document clarifying the procedure to be followed by interested parties for the submission of Community codes of conduct, and for their subsequent evaluation by the Working Party in accordance with Articles 27 and 29 of Directive 95/46/EC[3]. This document summarises the basic procedural steps to be followed in this context.

In June 2003 the Working Party adopted an opinion on the European Code of Conduct of FEDMA for the use of personal data in direct marketing; the Code is in accordance with Article 27 of the Data Protection Directive and provides sufficient added value to the Directive by being sufficiently focussed on the specific data protection questions and problems in the direct marketing sector and offering sufficiently clear solutions for the questions and problems at stake[4]. The Working Party considered that it therefore fulfilled the requirements laid down in Article 27 of the Directive.

The Working Party however underlined the fact that a general code like this can by definition not solve all specific problems inherent to the online world and therefore invites FEDMA to produce an annex to the Code dealing with these issues. This annex should in particular address the protection of children, who are especially vulnerable in the online context, as emphasised in the contribution of BEUC (the European Consumers' Organisation) which was consulted by the Working Party.

In a letter dated 16 December 2005, FEDMA submitted to the Article 29 Working Party a document containing an 'Annex to the Data protection and Direct Marketing Code' (hereafter 'the Annex'). According to FEDMA, the Annex is designed to cover specific concerns created by online marketing. As with the FEDMA Code, the intention is to neither supersede nor interfere in any way with national regulation, nor venture into areas which are not presently covered by EU legislation. The Annex aims at providing cross-border marketers with guidelines on how to behave when engaged in online marketing.

FEDMA sent a final version of the online marketing Annex in June 2010 which is finally in line with Directive 95/46/EC and provides sufficient added value.

CONCLUSION

The Working Party is satisfied that the online marketing Annex to the European Code of Conduct of FEDMA for the use of personal data in direct marketing is in accordance with Directives 95/46/EC and the currently applicable 2002/58/EC and the national legislation in place[5]. The Annex deals with a number of significant matters in the

[3] Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct, adopted on 10 September 1998, WP 13.

[4] Opinion 3/2003, Document WP 77, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp77_en.pdf

[5] National legislation may impose additional requirements.

particular field of the online sector (e.g. member-get-members campaigns, the protection of children, unsubscribe facility) and therefore provides sufficient added value to the Directives by offering clear solutions for the questions posed in the online marketing sector. It therefore fulfils the requirements laid down in Article 27 of Directive 95/46/EC. However, the implementation of Directive 2002/58/EC, as amended by Directive 2009/136/EC, in Member States' legislation may require the amendment of the Annex, particularly as far as cookies and spyware are concerned, in order to be in line with the new provisions. The Working Party recommends that FEDMA assess the adaptations that the Annex Code of Conduct will require as of 25 May 2011 in order to be in line with the legal framework resulting from Directive 2002/58/EC as amended by Directive 2009/136/EC and the national provisions implementing it.

In order to make sure that the national Data Protection Authorities are properly informed about the working of this Code in practice, the FEDMA Data Protection Committee will report annually to the Working Party about the application of the Code. Should this report give rise to questions, the Working Party will contact FEDMA in order to discuss the issues at stake.

The Working Party encourages FEDMA to promote this online marketing Annex Code of Conduct within the direct marketing sector in a proactive way, in order to ensure that data subjects are sufficiently informed about its existence and content, and to continue working in this field in order to continue increasing the standard of protection offered to individuals. The Working Party will pay special attention to the annual reports on the application of the Code to be provided by the FEDMA Data Protection Committee.

# Chapter Two
# Main Developments in Member States

# 2. Main Developments in Member States

## AUSTRIA

### A. New developments and activities

On 1 January 2010 the **Datenschutzgesetz Novelle 2010 (Data Protection Law Novella 2010)** entered into force. The main innovations adopted concern regulations with regard to video surveillance, the introduction of an obligation to notify serious cases of data protection breaches, and simplification of the notification of the use of data by changing to an online notification process.

The provisions on a simplified notification process were not yet applicable during the reporting period since, first, the technical prerequisites do not exist and secondly, these provisions will become available only once a new Data Processing Register Act has been passed and enters into force. An act of this type must be passed by 1 January 2012 at the latest.

Generally, it can be observed that through the explicit regulations on video surveillance in the Data Protection Law the general public is more aware that video surveillance involves use of data, and as a result, the number of notifications on this topic that are submitted to the Data Protection Commission has increased.

However, the amendment to the Federal Chancellor's standard and specimen ordinance excludes some types of video surveillance from the obligation to report to the Data Protection Commission. These include video surveillance at banks, jewellers, antique dealers, gold and silversmiths, newsagents and petrol stations, as well as video surveillance by owners of private developed land (single-family houses).

The Data Protection Commission has been critical of the draft of a **2010 administrative jurisdiction amendment**. This amendment provides that certain autonomous administrative bodies (including the Data Protection Commission) should be dissolved and their jurisdictional responsibilities transferred to newly created Administrative Courts. The Data Protection Commission highlighted, in particular, that the responsibilities granted by Article 28 of Directive 95/46/EC would have to be transferred to a new authority, since these activities cannot be exercised by Administrative Courts, considering that the latter would be competent only for decisions of a legal nature.

In 2010 the Data Protection Commission published a **brochure "Du bestimmst"** (You decide) as part of its efforts to **enhance awareness** about data protection; it was primarily aimed at young people, and provides information about the risks relating to data protection that arise when using new technologies (in particular the internet and social networks). The brochure is especially popular in schools, and the Data Protection Commission continues to receive requests for it.

The events for the 2010 European Data Protection Day were organised jointly by the Data Protection Council and the Federal Chancellery, and were primarily dedicated to the legal reforms in the area of data protection that came about as a result of the Lisbon Treaty.

| | |
|---|---|
| **Organisation** | Austrian Data Protection Commission |
| Chair and/or College | Chair: Dr Anton Spenling.<br>Executive Member: Dr Eva Souhrada-Kirchmayer.<br>College Members: Dr Anton Spenling, Dr Eva Souhrada-Kirchmayer, Mag. Helmut Hutterer, Dr Claudia Rosenmayr-Klemenz, Dr Klaus Heissenberger, Mag. Daniela Zimmer. |
| Budget | No own budget. Resources are covered by the Federal Chancellery budget. |
| Staff | 20 full-time posts (18 full-time and 4 part-time employees). |
| **General Activity** | |
| Decisions, opinions, recommendations | 61 formal decisions (complaints), 10 formal opinions, 22 authorisations (data transfer in third countries, research and surveys), 5 formal recommendations. |
| Notifications | 7 569 |
| Prior checks | 3 977 (notifications which are subject to prior checks). |
| Requests from data subjects | Writing: 913 (complaints excluded).<br>Phone: approximately 22 500. |
| Complaints from data subjects | Complaints leading to a formal decision: 94.<br>Complaints leading to a clarification or recommendation: 298. |
| Advice requested by parliament or government | This falls under the competence of two other institutions: the *Datenschutzrat* (data protection council) and the legal service of the Government in the Federal Chancellery. |
| Other relevant general activity information | 5 757 000 identifiers have been issued by the eGovernment register authority which is a part of the Austrian DPA. This authority is in charge and control of the sector-specific identity management used in the Austrian eGovernment. |
| **Inspection Activities** | |
| Inspections, investigations | 14: most of the cases are related to video surveillance. |
| **Sanction Activities** | |
| Sanctions | None. The Austrian DPA cannot impose sanctions.<br>One offence was reported by the DPA to the competent regional administrative authority that can impose sanctions. |
| Penalties | None. The Austrian DPA cannot impose penalties. |

| DPOs | |
|---|---|
| Figures on DPOs | None. The Austrian law does not foresee DPOs. |

## B. Case law

The Data Protection Commission pursued a complaint about radar monitoring by a municipality. The radar system was used for traffic monitoring, which was classified by the Data Protection Commission as a sovereign process. In this particular case, however, these kinds of traffic regulation measures did not fall under the municipality's legal competence; rather, these measures should have been introduced by state ordinance, but this did not exist. The decision was (recently) contested by the municipality in the Administrative Court; however, the complaint was rejected.

A complaint made by a student against the **electoral commission of the University of Vienna Students' Union** relating to an infringement of the right to anonymity of personal data when participating in the electronic vote for the Students' Union was rejected. The voting system encoded the identification data and the vote separately. As set out by the Data Protection Commission, comprehensive technical precautions had been taken, in order to prevent these data from being merged. Besides, the e-voting system also complied with the legal basis of the Students' Union Act.

A complaint was lodged against the "**Parliament** of the Austrian Republic". The complainant claimed that an infringement had been committed against his right to information, when his request for information on a member of the Austrian National Council, who was also a member of an **investigation committee**, was not fulfilled. Since the activities in a parliamentary investigation committee must also be classified as belonging to legislation, the Data Protection Commission had no jurisdiction and therefore dismissed the complaint.

**Google Street View** was registered with the Data Protection Commission at the beginning of 2010. When it emerged in spring 2010 that Google Inc. had also obtained **WLAN (WiFi)** data during its Street View drives and had even logged content data from e-mails and the like, an inspection procedure against Google Inc. was initiated. Google consequently deleted the content data.

The Head of the Data Protection Commission issued a notice on suspicion of infringing protected confidentiality interests and prohibited Google from any further use of Street View data. It was particularly unclear how the logging of WiFi data, which was not covered by the notification submitted to the Data Protection Commission, was connected to Street View. This decision of the Data Protection Commission was challenged by Google Inc. In the meantime Google has announced that it would not log any more WiFi data during Street View drives. Since it emerged in the investigation that the logging of WiFi data was conducted with a different purpose than for use in Google Street View and therefore could not be classified under the "Street View" data use, the notice was rescinded.

At the same time a "Procedure on checking registration" was initiated. This is permitted when circumstances that justify suspicions of a failure to register become known. In the meantime Google Street View was registered following improvements in the notification; at the same time several recommendations were made to Google Inc. by the Data Protection Commission. An investigation procedure in relation to the use of WiFi data by Google Inc. remained in progress.

## BELGIUM

### A. Summary of activities and news

#### Case Handling Workshop 2010

In March 2010 the Belgian Data Protection Authority hosted the 21st Case Handling Workshop at Le Square in Brussels. The following topics were discussed by the participants, primarily legal experts of the European DPAs: scientific research, direct marketing and mobility.

The Belgian DPA contributed to the discussions on scientific research with a presentation entitled 'Striking the balance between scientific freedom and data protection', which raised the following issues: the legitimacy of depositing and storing personal data in public and private archives, possible conditions for archive access, anonymous/encoded/non-encoded personal data.

#### 'Privacy and Scientific Research: from Obstruction to Construction'

On 22 and 23 November 2010, the Belgian Data Protection Authority organised an international conference, **'Privacy and Scientific Research: from Obstruction to Construction'**, dedicated to privacy and data protection aspects in scientific research. The event took place in the context of the Belgian EU presidency and was intended to create a dialogue between DPAs, national and international universities and researchers about best practices in both medical research and historical research. On 22 November, tutorials were organised to inform participants about relevant data protection legislation and specific medical and historical topics. This was intended to provide the necessary background for discussion workshops on 23 November, which led to a number of conclusions. More information about the conference, its results and follow-up activities can be found on the conference website (http://www.privacyandresearch.be).

#### Key topics – recommendations and opinions

In 2010 the Belgian DPA issued official documents on the following subjects: e-ticketing (Recommendation No 01/2010), Trusted Third Parties (Recommendation No 02/2010), mobile mapping technology (Recommendation No 05/2010), the fight against doping (Opinion No 08/2010), lifting bank secrecy (Opinion Nos 10 and 11/2010), the fight against marriages of convenience (Opinion No 12/2010) and the disclosure of electronic communications data to intelligence and security services (Opinion No 23/2010). All these documents, and more generally all opinions, recommendations and authorisations adopted in 2010, are available in French and Dutch on the Belgian DPA website, in the 'Decisions' section: (http://www.privacycommission.be/en/decisions/commission/)

#### 'I decide': awareness-raising website dedicated to young people and privacy

Considering the vulnerable position young people are often in as frequent users of new technologies, and following consultation with several stakeholders in education, the Belgian DPA started work on a specific website aimed at four target groups (children, young people, parents and education professionals) which was launched in January 2010. The aim of the website (in French http://www.jedecide.be and Dutch http://www.ikbeslis.be) is to promote the use of new technologies by young people while making them aware of these technologies' pros and cons.

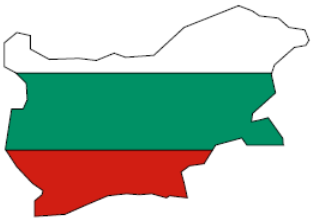
| | |
|---|---|
| **Organisation** | Belgian Data Protection Authority |
| Chair and/or College | Mr Willem Debeuckelaere<br>Composition of the college available at http://www.privacycommission.be |
| Budget | State grant established at EUR 5 516 000 for 2010.<br>Own income: EUR 60 000, specific agreement from the Belgian House of Representatives to assign an extra EUR 354 112.37 to organise a scientific conference, the case handling workshop and the Schengen inspections. |
| Staff | 56 |
| **General Activity** | |
| Decisions, opinions, recommendations | Commission: 25 opinions, 1 recommendation, 1 recommendation on further processing.<br>Sector Committees: 32 opinions, 209 individual authorisations, 4 general authorisations, 121 associations with general authorisations. |
| Notifications | Total: 11 269 notifications for 11 269 new processing operations, 261 modifications of existing processing operations, 73 corrections of existing processing operations, 376 terminations of existing processing operations. |
| Prior checks | N/A |
| Requests from data subjects | Received: 2 399 requests for information at back office and 3 008 at front office; Dealt with: 1 983 requests for information at back office and 3 008 at front office. |
| Complaints from data subjects | Received: 348; Dealt with: 190 |
| Advice requested by parliament or government | 87 |
| **Inspection Activities** | |
| Inspections, investigations | Cases opened: 85<br>Cases dealt with: 47 |
| **Sanction Activities** | |
| Sanctions | N/A |
| Penalties | N/A |
| **DPOs** | |
| Figures on DPOs | The function of DPO has been provided for by Article 17 of the Belgian Data Protection Act, but there is no Royal Decree implementing this Article yet. This document is currently under discussion at the Ministry of Justice. |

### B. Information on case-law

One sentence of the Ghent Court of Appeal was of particular interest for the Belgian DPA:

On 30 June 2010 the Ghent Court of Appeal decided that the Yahoo portal site, search engine and webmail provider cannot be forced to transmit the personal data of its e-mail service users to the Belgian judiciary. In the context of an investigation into cybercrime, the detectives of the Federal Computer Crime Unit (a specialised section of the Belgian federal police) monitored a group of swindlers using Yahoo e-mail addresses. Using companies' secret bank data, they ordered computers and other digital equipment. Yahoo refused to provide the personal data linked to these e-mail addresses to the Belgian authorities, arguing that Belgian law was not applicable since Yahoo did not have a subsidiary in Belgium, and no personal data were stored on Belgian territory. Furthermore, Yahoo referred to a treaty concluded between the US and Belgium requiring an intervention of the American authorities for this type of request. A Belgian court of first instance, however, did not accept Yahoo's arguments and in March 2009 it imposed on the company a EUR 55 000 fine, with a penalty of EUR 10 000 for every day the data were not transmitted. This sentence was subsequently quashed by the Ghent Court of Appeal.

## BULGARIA



### A. Summary of activities and news

#### A.1 Changes in laws

At the end of 2010 the Law for Protection of Personal Data was amended and supplemented concerning two main directions: strengthening the institutional competences of the Commission for Personal Data Protection (CPDP) and ensuring individuals' access to their personal data.

The legal amendments granted further powers to the CPDP with respect to the following:

- to assist in the implementation of state policy in the field of protection of personal data;
- to participate in the activities of international organisations concerning personal data protection;
- to participate in the negotiations and conclusion of bilateral and multilateral agreements on personal data protection;
- to organise and coordinate the training of personal data controllers in the field of personal data protection.

The second legal amendment, according to which free access to personal data is ensured, is in pursuance of a recommendation made under the evaluation of the state of preparedness of Bulgaria to join the Schengen area.

#### A.2 Activities related to Bulgaria's accession to Schengen

In compliance with the measures laid down in the National Schengen Action Plan, according to which Bulgarian state authorities undertake activities for ensuring the country's preparedness to join Schengen, in 2010 the CPDP launched an information campaign aimed at raising public awareness regarding data subjects' rights in the Schengen area. The information campaign included promotion of the CPDP website in the most-visited online media and on the websites of state institutions, as well as the printing and distribution of **40 000 leaflets** (20 000 in Bulgarian and 20 000 in different foreign languages), available at the most visible locations. This is the only measure in the National Schengen Action Plan targeted at civil society itself, and not limited to enhancing the country's administrative capacity.

As far as the CPDP inspection activity is concerned, in 2010 the Commission inspected **nine air carriers** in connection with the processing of passenger personal data and started with the organisation of inspections of key N.SIS personal data controllers. In relation to the implementation of the rules regulating the processing of personal data in the SIS, the CPDP experts appointed to deal with Schengen issues underwent training (organised by the Ministry of Interior) on the functioning of the Schengen information system.

At the end of 2010, the CPDP launched a procedure for the establishment of an EU Registry for classified information (already established), as well as a procedure for getting access to automated information systems and networks.

#### A.3 Opinions on key topics

In 2010 the Commission for Personal Data Protection was approached and issued opinions on many questions. Of significant public interest were the following opinions: the minimal technical requirements and the necessary documents needed in order for data transfer related to children awaiting adoption in third countries to be approved; the maintenance of a website for missing children – Bulgarian citizens; and the notification of a 'video surveillance' register in cases where data are processed during video surveillance activities.

| Organisation | |
|---|---|

| | |
|---|---|
| Chair and/or College | Commission, consisting of a Chair – Mrs Veneta Shopova, and four Members – Mr Krassimir Dimitrov, Mr Valentin Enev, Mrs Mariya Mateva and Mr Veselin Tselkov. |
| Budget | Allocated budget – BGN 2 650 000 (Bulgarian currency), executed budget – BGN 2 393 350. |
| Staff | Total staff number – 67:<br>49 persons employed under official (civil servant) relationship;<br>18 persons employed under labour relationship. |
| General Activity | |
| Decisions, opinions, recommendations | The Commission issued: 115 administrative acts in connection with submitted complaints; 22 mandatory directions (to data controllers in the areas of health, telecommunications, trade and services, transport and public administration); 46 opinions (upon request by personal data controllers regarding the application of the Law for Personal Data Protection, and in connection with normative acts that undergo an inter-institutional consultation procedure); 35 decisions permitting the transfer of personal data to third countries. |
| Notifications | 86 664 data protection controllers were added to the CPDP Register. |
| Prior checks | 1 432 |
| Requests from data subjects | 844 |
| Complaints from data subjects | 221 – mostly with regard to the 'telecommunications and information society' sector, and as regards 'financial, credit, leasing and insurance services'. |
| Advice requested by parliament or government | The CPDP produced opinions on primary and secondary legislative acts relevant to the Commercial Register, Bulgarian ID documents, the access to the National Population Data Base, the Internal Market Information System, and the functioning of N.SIS, as well as opinions on bilateral agreements in the police and judicial cooperation field. |
| Other relevant general activity information | Our authority carried out 6 training sessions for personal data controllers with a focus on the application of the provisions laid down in the Law for Protection of Personal Data.<br>Target groups were representatives of the local government and local administration, representatives of the national diplomatic service, heads of educational centres – the Balkan Institute for Labour and Social Policy, the National Union of Jurisconsults, and students.<br>Furthermore, the CPDP initiated and carried out an information campaign aimed at raising public awareness with regard to individuals' rights in the Schengen area. |
| Inspection Activities | |
| Inspections, investigations | Total number of inspections – 1 537 (mostly in the areas of health, trade |

| | |
|---|---|
| | and services, education, social services, tourism, etc.). |
| Sanction Activities | |
| Sanctions | The CPDP produced 1 511 statements of findings and 36 statements on ascertainment of an administrative violation. |
| Penalties | Fees and property sanctions in the amount of BGN 129 500 (imposed by our authority). |
| | |
| DPOs | |
| Figures on DPOs | N/A |

### B. Information on case-law

N/A

### C. Other important information

In 2010 the Commission for Personal Data Protection was approached to look into complaints mostly about violation of the individual's right to be informed when data concerning them is processed on the internet. The highest number of complaints was against service providers from the 'telecommunications and information society' sector (about disclosure of information to third parties for the purpose of debt collection), followed by the 'financial, credit, leasing, and insurance services' sectors.

A particular case related to the latter was the disclosure of a company's information on the Commercial Register comprising personal data that is deemed by our authority to exceed the purposes for which the Register was established. Furthermore, the disclosed personal information was not processed in accordance with the admissibility provision.

There was also an increase in the number of complaints concerning the processing of personal data by data controllers and also providers of direct marketing services.

Many complaints were lodged with the Commission for Personal Data Protection about denied access to personal information or about tacit refusal for such personal information to be provided to individuals. Our authority also ascertained violations related to breaches of the principle of proportionality, the principle of data processing for concrete and lawful purposes, and the processing of personal data without compliance with some of the applicable admissibility provisions.

After the final transposition of Directive 2006/24/EC into Bulgarian law in May 2010, the Commission for Personal Data Protection obtained a statutory power to monitor the security aspect of retained traffic data. Besides its competences under the law for Protection of Personal Data, the Law on Electronic Communications enabled the CPDP to: 1) demand, within its competence, that companies providing public electronic communication networks and/or services submit information; 2) produce mandatory instructions that require immediate execution.

## CYPRUS

### A. Summary of activities and news

In May 2010 Ms Panayiota Polychronidou was appointed Commissioner for Personal Data Protection. Ms Polychronidou succeeded Ms Goulla Frangou, who had served two terms in Office.

A draft bill amending Law 138(I)/2001 aiming to better implement the provisions of Directive 95/46/EC and to improve the effectiveness of enforcing the national data protection legislation, prepared by our Office, is currently in the pipeline.

In our Office's efforts to promote awareness, as part of the activities organised for the European Day for Personal Data Protection, our Office applied a budget of EUR 15 000 to distribute, on January 28, 42 000 information flyers to four daily newspapers' readers, covering approximately 93% of daily circulation. The same day, our staff distributed flyers and coffee mugs with a printed logo '28 of January European Day for Personal Data Protection' to Citizen Service Centers' (one stop shops) visitors, and answered citizens' questions on the protection of personal data.

Pursuant to the findings of the Inspector General's Report concluding that a number of persons receiving labour incapacity benefits/pensions from the Social Insurance Services (SIS) for medical reasons, among other things blindness, had been issued professional driving licences by the Department of Road Transport (RTD), our Office's advice was sought on how the Services concerned could exchange information, in line with the provisions of the data protection legislation, to avoid issuing professional driving licences to medically unfit persons. Taking into account the existing legislation regulating the competences of the SIS and the RTD and a relevant Opinion issued by the Attorney General of the Republic expressing the view that the issuing of a professional licence does not constitute proof of making use of the licence, the Commissioner informed the requesting parties that such incidents could be prevented by exchanging relevant information in the framework of a combination of their electronic filing systems, using a licence of the Commissioner issued in accordance with Section 8 of the Law. The combination would allow the RTD, upon receiving an application for a professional driving licence, to check, using the HIT/ NO HIT method, whether or not the applicant is receiving labour incapacity benefits/pensions from the Social Insurance Services (SIS) for medical reasons. If HIT is indicated, the RTD Director will subsequently ask the SIS for additional information relating to the medical reasons the applicant stated for receiving benefits/pensions and, if necessary, direct the applicant to the RTD Medical Board to check if the particular medical reasons should prevent him or her from obtaining a professional driving licence. In addition, the Commissioner expressed the view that technical restrictions should be put into place to ensure that RTD users can only access information relating to persons who applied for a professional driving licence and to prevent access to data relating to persons who receive benefits/pensions but who have not applied for a professional driving licence.

| | |
|---|---|
| Organisation | Office of the Commissioner for Personal Data Protection |
| Chair and/or College | Ms Panayiota Polychronidou |
| Budget | Budget allocated: EUR 318 091<br>Budget executed: EUR 235 487 |
| Staff | 7 Administrative Officers<br>2 Information Technology Officers<br>5 Secretarial Officers<br>2 Auxiliary staff |
| General Activity | |
| Decisions, opinions, recommendations | Number of opinions: 39 key topics |
| Notifications | Number of notifications: 222 |
| Prior checks | Number of prior checks: N/A |
| Requests from data subjects | Number of requests: N/A |
| Complaints from data subjects | Number of complaints: 804 |
| Advice requested by parliament or government | Number of requests for advice: 16 of the 39 opinions were issued pursuant to questions submitted by governmental bodies requesting advice. |
| Other relevant general activity information | Licences for the combination of filing systems: 32<br>Licences for the transmission of personal data to third countries: 33<br>Licences for the processing of sensitive data in the field of employment law: 0 |
| Inspection Activities | |
| Inspections, investigations | Number of inspections: 19 (18 in the banking sector and 1 of the Asylum Unit).<br><br>During 2010 our Office continued the inspections initiated in 2009 of 18 commercial banks that operate in Cyprus. In the course of the inspections, banks were asked to answer a model questionnaire, and various customers' application forms were scrutinised. In cases where the forms required customers' personal data, in breach of the principle of proportionality, the Commissioner recommended that these forms be amended to be in compliance with the Law. Pursuant to the findings of the answered questionnaires, the Commissioner issued Guidelines which focused on black lists, the criteria for different retention periods, |

| | |
|---|---|
| | particularly as regards banks' current and former clients, and the accuracy of data.<br><br>In the framework of an inspection decided on by the Eurodac Coordinated Supervision Group in December 2010, our Office asked the Asylum Unit to complete and return a relevant questionnaire prepared by the Group, which aimed at checking national practices as regards advance deletion and the verification of minor asylum applicants' age and the Unit's compliance with the relevant provisions of Regulation (EC) 2725/2000. |
| Sanction Activities | |
| Sanctions | 14 |
| Penalties | 12 penalties (total of EUR 17 000) |
| DPOs | |
| Figures on DPOs | N/A |

## CZECH REPUBLIC

### A. Summary of activities and news

In 2010 the Office for Personal Data Protection ('OPDP' or 'the Office') entered the 11th year of its existence and work, and it was President Mr Igor Němec's first year after his re-election (for a new period of five years).

The most important event was the **European Data Protection and Privacy Commissioners´ Conference** hosted by the OPDP on 29 and 30 April in Prague. Under the challenging motto 'Weighing up the past, thinking of the future' the conference was divided into four sessions: 'Internet of things: ubiquitous monitoring in space and time', 'Children in a cobweb of networks', 'Personal data protection at the crossroads', 'Public sector: respected partner or privileged processor?', and one special panel on ethnic profiling. Four resolutions were adopted – on body scanners for airport security purposes, on the envisaged agreement between the European Union and the United States of America on data protection standards in the area of police and judicial cooperation in criminal matters, on future development of data protection and privacy, and on the setting up of joint actions of awareness and education of youngsters at a European and international level (see more details at http://www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=690&lang=en ).

In the framework of the Government legislation procedure, the Office is mandatorily addressed with requests for comments. This is why also in 2010 an important part of the Office´s legislative activities concerned specific law with impacts on privacy and personal data protection. One of the most important tasks in which the Office was involved was the work of an expert group concerned with developing a legal regulation on processing samples of human DNA. The Czech Republic is still largely without specific legislation on police DNA databases, where processing of DNA by the police can currently be regulated to a considerable degree by a mere order of the Police President. Similarly, the Czech Republic also lacks robust specific legislation concerning the use of camera surveillance systems, in relation to which the Office commented on a draft legal regulation that was not finalised in 2010. The Office considered it more suitable to proceed solely with legal regulation of the frequently problematic and discussed cases of cameras used on publicly accessible places and premises.

From the viewpoint of the competence of the Office and its activities, particularly in the area of electronic communications and services in the information society, of fundamental importance in 2010 was the commencement of the implementation of Directive 2009/136/EC. The Office submitted a number of comments on the Electronic Communications Act (for which it also supervises the personal data protection aspects).

Among many other drafts commented on, the draft amendment to the Criminal Records Act is of particular significance.

At the end of 2010, the Office received a request for its opinion on the draft **Government Strategy of Combating Corruption** for the period 2010-12 containing a number of legislative measures directly concerning the personal data protection issue. In general the Office noted that specific measures must respect the principles of personal data protection and thus need to be formulated in detail so as to allow for processing and disclosing personal data only for precisely specified purposes, and that they are available only to clearly delimited authorised bodies, under precisely specified procedures and to an extent absolutely necessary for fighting corrupt practices. Specific objections were raised e.g. in relation to measures such as the register of misdemeanours where the Office pointed out that it was not entirely clear why it was necessary to fully centralise the records of misdemeanours in various areas of human life, and noted that the regime of the register of such sensitive data had to contain adequate guarantees, similar to the strict model of criminal records. Some comments concerned the reliability tests for persons working in public authorities and the central register of accounts.

In 2009, the OPDP was granted new competences and assigned tasks which started and were developed in 2010: to create (by June 2012) and then to carry out the ORG Information System as part of the system of Basic Registers related to the **eGovernment programme**. The ORG IS, co-financed by the EU, will serve as an identifier converter by replacing the currently used universal 'birth identification number' with a system of meaningless identifiers differing for the individual agendas or groups of agendas.

The amount of money allocated from the state budget for the above-mentioned specific eGovernment programme task (ORG IS agenda) is not included in the amount indicated in the summary table below.

| Organisation | |
|---|---|
| Chair and/or College | Igor Němec, President of the OPDP |
| Budget | Total expenditure: about CZK 97 million, i.e. approximately EUR 3.9 million |
| Staff | 97 employees: 61.5% with university education, 51% being women |
| General Activity | |
| Decisions, opinions, recommendations | 2 opinions (on transfers of data abroad, on PDP aspects of private detective services).<br>10 standpoints on currently important subjects, published on websites or in bulletins (e.g. on DNA). |
| Notifications | 4 037 |
| Prior checks | 64 (proceedings related to notifications) |
| Requests from data subjects | 3 822 enquiries and requests for consultations by citizens |
| Complaints from data subjects | 1 039 complaints and instigations pursuant to the PDP Act, plus<br>2 834 complaints and instigations related to unsolicited commercial communications |
| Advice requested by parliament or government | 217 |
| Other relevant general activity information | 317 consultations for legal persons<br>219 consultations for natural persons operating a business |
| Inspection Activities | |
| Inspections, investigations | 106 inspections related to the PDP Act,<br>plus<br>163 control proceedings related to unsolicited commercial communications |
| Sanction Activities | |
| Sanctions | 209 financial sanctions totalling EUR 254 000, of which EUR 19 600 related to unsolicited commercial communication; financial sanctions are mostly accompanied by ordering measures. |
| Penalties | (see also above – financial sanctions)<br>The highest penalties were imposed in the public sector (central registers of medication, students, inhabitants: EUR 92 000, 32 000, 16 000 respectively).<br>In the private sector, the highest penalties did not exceed EUR 7 200 per |

| | |
|---|---|
| | case (hotels, cameras in shops and in lodging houses, etc.). |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

The Czech Republic is not a typical country for legislation based on case-law, in the sense of precedent decisions by courts.

In personal data protection legislation, the jurisdiction of courts is quite important anyway because law courts have a role of second instance for complaints against the decisions of the OPDP (first instance is the President of the Office) and anybody can also bring a case before the court directly.

In 2010 there were 18 new actions lodged in the field of personal data protection. Seven actions against the Office´s decisions were dismissed by the court and six decisions of the Office were cancelled by the court.

As an example, the following are the three typical judgements, all of them regarding a complaint against the Office´s decision, where the actions were dismissed:

- the judgement of the Municipal Court in Prague (11 Ca 433/2008-89) on the privacy protection versus protection of ownership issue, related to a camera system in a hotel;
- the judgement of the Municipal Court in Prague (9 Ca 4/2008-33) on the processing of personal data by a travel agency;
- the judgement of the Supreme Administrative Court (1 As 93/2009-121) related (in general) to the nature of control and administrative procedures.

## C. Other important information

In 2010, the OPDP recorded a decreasing number of applications for **authorisation to transfer personal data to third countries.** This trend was caused particularly by the fact that the controllers increasingly used instruments created by the European Commission for securing adequate protection in third countries, mainly the standard contractual clauses and the 'Safe Harbour' regime in the United States. Nevertheless controllers most often rely on the provision of the DP Act allowing transfers on the basis of the data subject´s consent or instruction, which still need authorisation by the Office.

In its **international cooperation activities** the Office continued to take part in the work of the Article 29 Working Party on Data Protection and several of its subgroups. The President of OPDP Mr Igor Němec was elected Vice-Chairman of the Article 29 Working Party at its 77th session in October 2010.

The Office, and its experts in particular, were asked to join several international teams under EU-funded projects in countries introducing or improving their personal data protection. One of the Office´s lawyers, Mr Jiří Maštalka, became the key expert in a project in Albania, and the Office nominated four short-term experts for a similar project in the FYROM. Practical findings obtained in the Office´s supervisory procedures were presented to Bulgarian colleagues at the two-day workshop in Prague. The Office´s experts also shared with their Polish and Hungarian colleagues common work funded under the EU Leonardo da Vinci programme.

The OPDP focused its **awareness-raising activities** and its communication with the media on active daily service and provision of up-to-date information through its website and by organising press conferences. The interest among journalists in press conferences was quite satisfactory: the conferences were attended by about 20 to 25 journalists and a whole range of media representatives was represented – agencies and electronic and press media. The number of reports published in the media in respect of personal data protection as a follow-up to the press conferences was some 30 to 60 in three days after the press conference. In annexes to press releases, the Office regularly provides information on investigations closed by initiation of administrative proceedings to impose fines.

At the winter press conference, traditionally organised on the occasion of Data Protection Day, the Office launched the fourth competition for children and youth called 'My privacy! Don't look, don't poke about', which aimed this year to draw the attention of children and young people to the risks connected with communicating through the internet and utilising social networks.

## DENMARK

### A. Summary of activities and news

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | The day-to-day business of the DPA is attended to by the Secretariat, headed by a Director.<br><br>Cases of significant interest (approximately 15 cases per year) are put before the Council for a decision. The Council is chaired by a Supreme Court Judge. |
| Budget | DKK 20.3 million |
| Staff | Approximately 35 |
| **General Activity** | |
| Decisions, opinions, recommendations | N/A (included in figures below) |
| Notifications | 2 660 |
| Prior checks | 2 660 |
| Requests from data subjects | 2 018 (requests and complaints) |
| Complaints from data subjects | N/A |
| Advice requested by parliament or government | 383 |
| Other relevant general activity information | 52 cases relating to security |
| **Inspection Activities** | |
| Inspections, investigations | 64 |
| **Sanction Activities** | |
| Sanctions | Each year the Danish DPA expresses criticism of several data controllers for not complying with the Act on Processing of Personal Data. |
| Penalties | Fines in 3 cases. |
| **DPOs** | |
| Figures on DPOs | N/A (this is not an option according to Danish legislation). |

## B. Information on case-law

### Public authorities and SMS communication

In 2009 the Danish DPA was contacted by the Copenhagen Municipality regarding the use of cell phone text messages from the municipality to its citizens. Initially the municipality wanted to remind people of their appointments with the city's administration.

The Danish DPA stated that in the DPA's view communication over the cell phone network is not a safe way of communicating and therefore it is not permitted for the Government to send sensitive and/or confidential information to a person's cell phone.

With this as a general rule, in 2010 the Danish DPA opted for an exception if certain guidelines are followed.

These are:

- The guidelines are only reminders and other service messages are allowed to be sent in this way.
- The citizen must have accepted this form of communication beforehand.
- Personal identification numbers are not allowed in the messages.
- People are only allowed to receive information regarding themselves or their children.
- The technical solution must ensure that the phone number used to communicate is correct.

The Danish Government has developed a technical system called nemsms which is part of the Government's communication system.

### Cloud computing

In 2010 the Danish DPA received an inquiry from Odense Municipality regarding the use of the Google Apps online office suite with calendar and document processing features.

Odense Municipality wanted teachers to use the solution when registering information about lesson planning and assessments of lesson plans and individual students' educational development. In addition, the teachers would take notes about classes and students' cooperation, and prepare letters to parents regarding their children. They also wanted to use the solution for planning and sending invitations to meetings and distributing information about school-related activities.

This would have involved sensitive information including: data concerning health, serious social problems and other purely private matters.

The Danish Data Protection Agency discussed the matter in a meeting of the Data Protection Council.

The Danish Data Protection Agency saw problems in a number of areas in relation to the requirements of the Act on Processing of Personal Data and the Executive Order on Security. Thus, the Danish Data Protection Agency did not concur with Odense Municipality's assessment that confidential and sensitive data about students and parents can be processed in Google Apps.

These problems included:

- the transmission of data to third countries;
- general information on processing security in connection with Odense Municipality's use of the Google App;
- the regulations of the Act on Processing of Personal Data regarding data protection requirements when using an external processor;
- deletion of personal data;
- transmission and login;

- control of rejected attempts to access data;
- logging.

The Danish Data Protection Agency is willing to reconsider the case for a revised statement if Odense Municipality continues work on the case and seeks solutions to the identified issues.

### C. Other important information

In the Thirteenth Annual Report, the Danish DPA reported that a new Danish bill regarding mandatory video surveillance in taxis was about to be introduced in the Parliament. As a follow-up, the Danish DPA can report that the law was passed by the Danish Parliament on 22 April 2010 and entered into force on 1 July 2010.

# ESTONIA

## A. Summary of activities and news

The scope of personal data protection in Estonian legislation covers all sectors of society. It also covers all private persons who process the personal data of others outside the private sphere (e.g. on the internet). All institutions and also all persons in private law that perform public functions or use public funds are possessors of public information.

The Estonian Data Protection Inspectorate (EDPI) is a small authority with 17 employees. Inevitably it raises questions such as how can we be influential in our area of responsibility regardless of our quantitative indicators? So in the last few years we have made radical changes in our action strategy.

The first thing we decided to do was to accelerate the reacting activities (registration, requests for explanations and reviews of complaints) in order to increase the scope of supervision of our own initiative and other proactive activities. The following are examples:

- from 2008 to 2009, we launched a major action to call on processors of sensitive personal data to comply with the notification obligation, which means that less supervision is required in this area now;
- the helpline cuts our workload, as answering simple questions by phone is less time-consuming than correspondence;
- we introduced a simplified supervision procedure with regard to less complicated problems;
- we use risk-based gradation of measures when we react to breaches.

Getting the volume of reacting work under control allows us to act as a strategic regulator:

- we intervene on our own initiative where risks are higher and intervention has a greater impact;
- we use new forms of supervision: extensive comparative monitoring and audits that allow us to see the big picture;
- instead of 'retail training', we focus on the preparation of guidelines and 'wholesale training';
- we improve the efficiency of cooperation;
- we improve the efficiency of our media work.

The activities of the EDPI in recent years are partially illustrated in the table below. The volume of explanatory and counselling work (requests for explanations, helpline) has stabilised compared to indicators from the previous years. However, the number of complaints and challenges has doubled. In our opinion, this increase has not been caused by a sudden deterioration in the area of information law, but by the fact that people are better informed about their rights.

The number of rulings has almost trebled due to the increase in the number of complaints and challenges as well as the new form of supervision – comparative monitoring. Tens or hundreds of objects of monitoring are reviewed in one monitoring session and we react to serious omissions with recommendations and rulings. We launched three monitoring sessions in 2009 and completed six such sessions in 2010.

Compliance and adequacy audits are also a new form of supervision, and we initiated four audits in 2010. These audits give us a comprehensive picture of the compliance of large and sensitive information systems with personal data protection requirements. We use international methodology to conduct these audits.

Notification of sensitive personal data processing moved largely to the internet at the end of January 2010. Automatic error filters and the standard forms based on the type submitted make it easy for both the sender and the recipient. The orders issued to those who ignore the registration obligation are also standard. This is why we transferred the notification to our administrative department, as it allows our main departments to focus on more specific work.

Last year we issued five personal data protection and public information guidelines – Publication of Payment Defaults Data, Using of Personal Data in Election Campaigns, Data Transfer to Foreign Countries, Guideline to the Holders of Information who are Private Legal Persons and General Guideline on the Public of Information.

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | Dr Viljar Peep |
| Budget | EUR 551 190 |
| Staff | 17 officials |
| **General Activity** | |
| Decisions, opinions, recommendations | 5 guidelines on data protection and freedom of information |
| Notifications | 468 notifications on the processing of sensitive personal data |
| Prior checks | N/A |
| Requests from data subjects | 893 requests in writing and 1 061 requests by phone |
| Complaints from data subjects | 592 complaints and challenges |
| Advice requested by parliament or government | 21 opinions on the draft legislation |
| Other relevant general activity information | 139 approvals on public sector databases |
| **Inspection Activities** | |
| Inspections, investigations | 5 comparative monitorings, 6 audits and 58 on-site inspections |
| **Sanction Activities** | |
| Sanctions | 203 orders<br>35 misdemeanour proceedings |
| Penalties | 15 penalty payments and fines imposed by EDPI – altogether EUR 13 470 |
| **DPOs** | |
| Figures on DPOs | 156 DPOs appointed in 2010 |

## B. Information on case-law

### The issue of private life in employment relationships

The issue of the personal data of employees has been the priority of the EDPI in recent years. This covers the collection and use of the data of jobseekers, employees and former employees, and background checks concerning employees.

The legal basis for this is found in the Employment Contracts Act of Estonia, which stipulates that an employer who prepares an employment contract may only ask a person for information with regard to which the employer has a legitimate interest. During the employment relationship, the employer must respect the privacy of employees and verify the performance of their duties in a manner which does not violate the employee's fundamental rights. Also, the Personal Data Protection Act of Estonia stipulates the general principles (purpose limitation, proportionality, etc.).

However, these are just the general principles. When we started a discussion about their implementation in real life, the only more or less clear and unanimous opinion was that employees may not be observed on camera in toilets and shower rooms.

Hundreds of practical questions were raised in the course of the discussion: How can the background of jobseekers and employees be checked? Who may read e-mail messages containing the employee's name and the employer's domain name? How can the health of employees be checked? What about the issue of video surveillance of employees, etc.?

There were also disputes about fundamental issues of the theory of law. For example, when does an employer process the personal data of an employee on the basis of the latter's consent (consent may be withdrawn), and when may it be done to guarantee performance of the employment contract?

We discovered that there was no legal foundation on which we could build our simple summary. There was no basic legal analysis conducted in Estonia, as legal literature only covered a few aspects, and national court practice offered even less. Finally, we decided to discuss the subject of protection of private life in employment relationships at our annual conference on 27 January 2010, and later at a roundtable for employers and central employee organisations, which was attended by other agencies and experts. Personal Data Processing in Employment Relationships was finally ready for publication on 24 January 2011.

## C. Other important information

### Cooperation with database keepers

Since 2010 the EDPI has strengthened cooperation with the largest data processors and database keepers in Estonia. The more sensitive the information contained in a database, the stronger the internal control measures that the keeper of the database must apply regarding the use of such information. For example, internal control of the use of the Population Register is relatively efficient – the EDPI is informed of any suspected cases of misuse.

Management of information assets, including granting of access rights, was centralised in the Police and Border Guard Board after the merger of the agencies, and the internal control system of the merged agency was made more efficient. The EDPI advises other agencies that keep large and sensitive databases to look into the implementation of a similar model.

Zero tolerance was established with regard to persons who misuse the police database, and anyone doing so is punished with disciplinary as well as misdemeanour procedures. There is regular information exchange between the police and the EDPI for this purpose. This has brought about a noticeable change for the better within the organisation.

Also, we have launched cooperation in the area of e-health, similar to the internal control of the previously mentioned databases.

## FINLAND

### A. Summary of activities and news

The Office of the Data Protection Ombudsman proactively addressed a drastic change in our operational environment. The office's tasks are increasing while at the same time the national productivity programme has reduced our resources. Our office has improved our extensive system of guidance, planning and monitoring in order to increase its efficiency. In order to ensure the commitment of all staff, together we renewed our vision, operational plan, values and strategy. Our vision outlines our objectives, our operational plan defines the way we act, our values guide our decision-making, and our strategies guide the means that we use.

In accordance with our goals, the office's main emphasis was preventive operations. Aiming to have an influence on the public, we focused on giving appropriate advice and guidance and integrating into working groups and committees, which are significant in the field of data protection. We are involved in about 80 different working groups.

Data management was the central theme of our guidance operation. Finland has introduced a special accounting information procedure, which serves the leadership of organisations in their management and reporting activities, and at the same time allows the Data Protection Ombudsman to more efficiently carry out law enforcement activities.

In Finland, in addition to the European Data Protection Day, a special national data security day is held as part of the national information security strategy. The goal is to improve citizens' awareness of security threats and improve their level of knowledge about the means that can be used to combat threats and how data subjects can protect their rights.

Our office had extensive cooperation with different interest groups. Various data protection steering groups operated in, among others, the sectors of public health care, social welfare, telecommunications and education. Also during the year, a new Data Protection Ombudsman's office and business life joint steering group was born, which focused on topical data protection issues related to marketing and consumer relationship management. The first private-sector-organised networks of data protection experts also started operating.

A law approved by Parliament concerning electronic identification came into force. At the same time the special Identity Management Group, in connection with the Ministry of the Interior, proposed clarification of the criminalisation of identity theft.

Finally, after the Taxation Data and Mass Media judgment, the Personal Data Act, which implements Data Protection Directive 95/46/EC, was amended upon the initiative of the Ministry of Justice.

The following table summarises significant figures related to the Office of the Data Protection Ombudsman.

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | Reijo Aarnio has been the Data Protection Ombudsman since 1 November 1997 |
| Budget | The overall annual budget is about EUR 1 541 403 |
| Staff | The total number of staff is 20 |
| **General Activity** | |
| Decisions, opinions, recommendations | 2 601 |
| Notifications | 284 |
| Prior checks | See notifications |
| Requests from data subjects | 881 |
| Complaints from data subjects | (access and rectifications) 174 |
| Advice requested by parliament or government | 110 |
| Other relevant general activity information | Cooperation work with data controllers in the following sectors:<br>Education, Health Care, Social Affairs, Telecommunications, Employment and Economy. |
| **Inspection activities** | |
| Inspections, investigations | 1 972 |
| **Sanction activities** | 82 |
| Sanctions | N/A |
| Penalties | N/A |
| **DPOs** | >1 000 |
| Figures on DPOs | |

## B. Information on case-law

### Privacy

The Supreme Court convicted the authors of the book Prime Minister's Bride for spreading defamatory information about the Prime Minister's private life. The Supreme Court held the author and the publisher responsible because in the book they had published details about the most fundamental part of the Prime Minister's private life and information about private events. The Supreme Court pointed out that a person's position as Prime Minister and the ability to wield significant political power means that the protection of his or her private life is typically narrower than a private person's. However, even a leading politician's private life and particularly the fundamental part of it cannot remain unprotected (Supreme Court 2010.39).

The Supreme Administrative Court resolved a matter concerning the results of an aptitude test. X and Y had both applied for the post of Director. Upon Y's election to the post, X requested the results of Y's aptitude test. X asked for the information under Section 11 of the Openness of Government Activities Act because Y's aptitude test could have had an effect on the resolution of a matter concerning X. However, giving X information relating to Y's aptitude test would have been contrary to an important private interest, according to the Supreme Administrative Court. The Court referred to the Government proposal which stated that making the results of aptitude tests public is contrary to the human right of protection of privacy (Supreme Administrative Court 2010:60).

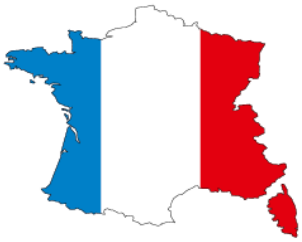
### Data Protection

The Supreme Administrative Court ruled on the matter of the police’s right to information from the Social Insurance Institution, concerning an individual's medicine purchases, for use in a police investigation of a suspected murder. The Supreme Administrative Court authorised police to obtain the information under Section 35 of the Police Act (Supreme Administrative Court 2010:42).

An applicant asked the Data Protection Board whether information concerning the repair history of motor vehicles is to be considered personal data under Section 3 of the Personal Data Act. The applicant asked for permission to process this information in order to create a new database to handle, maintain and share the information. The Data Protection Board rejected the application because the processing failed to meet the requirement of accuracy, since erroneous, incomplete or obsolete data could be processed, and the requirement of exclusivity of purpose, because this additional processing was not defined before the collection of the data. According to the Data Protection Board, licence plate numbers are to be considered personal data (Data Protection Board 2/932/2009).

The Turku Administrative Court upheld the Data Protection Board's ruling prohibiting a corporation from processing and submitting, through an SMS service, data relating to earned and capital income of natural persons, in the Taxation Data and Mass Media (Veropörssi) case (Administrative Court of Turku 10/0846/2).

# FRANCE



## A. Summary of activities and news

### Young people are an important target group for the CNIL

Young people are the main players in today's digital world, and that of tomorrow. In 2010 the National Commission for Information Technology and Civil Liberties (CNIL) decided to make enhancing awareness among young people and education professionals one of their priorities.

For this reason it made unprecedented efforts to help them by dedicating more than EUR 500 000 to a campaign that involved, in particular, the publication of two special editions of newspapers dedicated to 10-14 year olds and 14-18 year olds on the topic of protecting one's privacy on the internet.

### The CNIL is a pragmatic authority

The CNIL is convinced that the spread of a culture of information technology and civil liberties is brought about by providing a better service for users. Consequently, it now offers the option of carrying out the formalities in advance online, and also of submitting a complaint directly online. Today, almost 20% of the complaints are sent to the CNIL in electronic format in this way.

The CNIL has also implemented a policy of extremely active monitoring.

As a result, in 2010, when the legal framework for monitoring was specified[6], the number of checks undertaken rose to 308, compared with 270 in the previous year. Particular attention was given to the checks on video surveillance systems subject to the Law on Information Technology and Civil Liberties. Consequently, 55 checks were carried out on these systems. Many shortcomings were discovered; in particular, these related to failure to make a declaration, disproportionate data processing, retaining images for an excessive period of time and even failure to provide the required information or security.

The CNIL is also an authority that has adopted recommendations or decisions in new situations posed by online gaming, electronic voting or even by digital applications for the administrative and educational management of pupils.

This pragmatism and this desire to stay as close as possible to practices is based on the work done by the expert service of the CNIL which has been strengthened in terms of its workforce and which is monitoring the most recent developments in the area of new technologies; the CNIL can therefore anticipate and be in a position to advise companies about new situations.

### The CNIL is a forward-looking authority

In order to better identify and anticipate changes and to deal with the major developments in new technologies which can impact the protection of personal data, a new department has been created in the CNIL: the Department of Research, Innovation & Foresight (*Direction des Études, de l'Innovation et de la Prospective* – DEIP).

It is this same concern to influence the future of data protection that causes the CNIL to be particularly active in the revision of Directive 95/46.

[6] See the two rulings of the Council of State, No. 304300 and No. 304301 of 6 November 2009 – the Council of State decided to annul two penalties imposed by the CNIL on the grounds that the spot checks, on the basis of which the penalties were imposed, breached the regulations as they did not provide sufficient information to those responsible for data processing. Since then, the CNIL has had to modify its practices and, now systematically informs persons subject to spot checks about their right to refuse the check.

| | |
|---|---|
| **Organisation** | *Commission Nationale de l'Informatique et des Libertés* – CNIL (France) |
| Chair and/or College | Chairman: Alex Türk.<br>Vice-Chairpersons: Isabelle Falque-Pierrotin, Emmanuel de Givry.<br>Composition of the college: 4 Members of Parliament / 2 Members of the Economic and Social Council / 6 Supreme Court Judges / 5 qualified personalities appointed by the Cabinet (3), the Chairman of the National Assembly (1) and the Chairman of the Senate (1). |
| Budget | Total credits for 2010: EUR 14.7 million |
| Staff | Number of staff: 148 |
| **General Activity** | |
| Decisions, opinions, recommendations | 1 659 decisions / opinions / recommendations |
| Notifications | 68 863 notifications to the CNIL |
| Prior checks | Request for authorisation: 1 682 requests for authorisation and 4 273 requests for authorisation with the commitment of data controllers to comply with a single decision of the CNIL.<br>Authorisations: 1 346 authorisations and 4 273 authorisations delivered after receiving the commitment of data controllers to comply with a single decision of the CNIL. |
| Requests from data subjects | Requests from the public: 28 490 written requests and 10 000 calls per month.<br>Requests from data subjects: 1 877 requests for indirect access where processing involves State security, defence or public safety. |
| Complaints from data subjects | 4 821 complaints from data subjects (Labour: 20%, Bank: 20%, Business: 20%, Internet / Telecoms: 20%, Health / Social: 5%, Others: 15%). |
| Advice requested by parliament or government | 8 opinions on regulations.<br>78 opinions on the implementation of data processing on behalf of the State. |
| Other relevant general activity information | EUR 500 000 on public awareness campaign |
| **Inspection Activities** | |
| Inspections, investigations | 308 investigations (Biometrics: 54, Marketing: 78, Police files: 40, New technologies: 12, Data security: 15, Services to population: 10, Labour: 91; Others: 8) |
| **Sanction Activities** | |

| | |
|---|---|
| Sanctions | Sanctions imposed by the CNIL: 4<br>Legal actions against data controllers: 118 (Orders issued: 111, Warnings: 4, Emergency procedure: 3) |
| Penalties | Total amount EUR 32 500, imposed by the CNIL |
| DPOs | |
| Figures on DPOs | 7 300 organisations appointed a DPO |

## GERMANY

### A. Summary of activities and news

Even after the amendment of the Federal Data Protection Act (BDSG) in 2009 the discussion about the necessary modernisation of data protection law in Germany continued. In March 2010 the Conference of the Data Protection Commissioners of the Federation and of the *Länder* adopted a key issues paper 'A modern data protection law for the 21st Century'. The key issues paper serves as a contribution to the discussion about reform of the national data protection law and contains important basic principles for modernising the data protection law.

Individual amendments in the BDSG entered into force in 2010:

- As regards rating agencies and the determination of score values, improved data protection rules apply from 1 April 2010 (Section 28b of the BDSG) and now determine more precisely which personal data may be transferred concerning a claim made to a rating agency. In addition, for the first time, the conditions for the application and implementation of a scoring procedure have been defined by law. The data subjects' rights to information have been strengthened: in particular, now there is a right to free information on which score values were transferred to third parties and how the individual score had been calculated.
- Through the implementation of the Consumer Credit Directive, which entered into force on 11 June 2010, the BDSG now ensures the equal treatment of European lenders concerning access to domestic rating agencies (Section 29, paragraph 6 of the BDSG).
- More transparency is provided by the new regulation according to which the consumer is to be notified immediately if, in connection with consumer loan contracts or contracts concerning financial assistance for payment, his or her request for a loan is refused because of a (negative) query at a rating agency (Section 29, paragraph 7 of the BDSG).

In the year being reported on, almost all Federal States (*Bundesländer* or *Länder*) launched their respective activities to achieve the complete independence of the data protection supervisory authorities in the non-public sector as required by the European Court of Justice (Judgment of 9 March 2010 – C-518/07). In the overwhelming majority of the *Länder* it is envisaged to assign the supervision of the non-public sector to the data protection commissioners of the *Länder* unless this has already happened. The executive branch may not exercise any influence over the data protection authorities. Therefore, the data protection authorities must have the necessary decision-making authority in matters of personnel, budget and organisation. However, the full consequences of the judgment of the ECJ on the position of the Federal Commissioner for Data Protection and Freedom of Information in Germany are yet to be seen. Even if the judgment refers explicitly only to the supervision of data protection in the *Länder*, the principles emphasized in the judgment are also applicable in respect of the supervision of data protection at the federal level.

As in previous years, in 2010 a sharp increase in the workload and tasks was registered: for instance, the number of complaints received in my office increased from 5 066 in 2009 to 6 087 in 2010. Therefore, it is all the more gratifying that in the financial year 2010 my office was granted 12.5 new staff posts. With this, the number of staff members increased from 69 to 81. The additional number of staff members allows my office to better cope with existing legal tasks concerning carrying out inspections and providing consulting related to data protection law, as well as to take up new tasks proactively. Thus, this made it possible to expand in particular the competence in technological data protection and to strengthen my monitoring and supervisory work. I have also expanded my offer of information to the public, e.g. through new thematic flyers and through a short film on my web page about the importance of data protection and about the tasks of my office.

In my 23rd activity report covering the years 2009 and 2010 you will find more details on my activities in 2010. You will find this activity report on my website under http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TB_node.html and my press release about this report in English under

http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2011/23rdActivityReport.html?nn=410156.

Please note: In Germany there is not only the Federal Commissioner for Data Protection and Freedom of Information acting as Data Protection Authority; at the level of federal states (*Länder*) there are the offices of the *Länder* Data Protection Commissioners and – in some federal states – separate supervisory authorities with regard to the private sector.

The following table refers to the office of the Federal Commissioner for Data Protection and Freedom of Information only.

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | Peter Schaar, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* [BfDI]) |
| Budget | EUR 6.5 million |
| Staff | 81 |
| **General Activity** | |
| Decisions, opinions, recommendations | N/A |
| Notifications | N/A |
| Prior checks | N/A |
| Requests from data subjects | 13 257 |
| Complaints from data subjects | 6 087 |
| Advice requested by parliament or government | N/A |
| Other relevant general activity information | In December 2010 the Binding Corporate Rules of the Deutsche Post AG were adopted |
| **Inspection Activities** | |
| Inspections, investigations | 52 |
| **Sanction Activities** | |
| Sanctions | 30 complaints (2009 and 2010) according to Section 25 of the Federal Data Protection Act |
| Penalties | N/A |
| **DPOs** | |
| Figures on DPOs | N/A |

## B. Information on case-law

### Decision of the Federal Constitutional Court on the retention of telecommunications traffic data:

Already in 2008, through two decisions in the provisional legal protection proceedings, the Federal Constitutional Court strictly limited the use of data retained for later use. Through the judgement of 2 March 2010 the Federal Constitutional Court declared the statutory provisions on data retention unconstitutional and therefore null and void. Through this, the largest mass constitutional complaint in the history of the Federal Republic of Germany with more than 35 000 appellants turned out to be successful.

While the Court on the one hand revoked the German Implementation Act as it was unconstitutional, in this context the Court explained on the other hand that six-month storage of personal data without any cause was only strictly prohibited if this happened for vague and not yet defined purposes. Thus, a constitutional implementation of the European Directive on Data Retention would be possible in principle. However, this is subject to very strict requirements because the intrusion into private telecommunications related to data retention was deemed extremely serious.

With regard to a possible review of the law, the court designated four areas that need to be adhered to for a constitutional concept of data retention. In addition to a high standard of data security, adequate transparency and an effective system of legal protection, the legislator must above all stipulate by law clear rules on the scope of the use of data.

In addition, the court stated that in general, precautionary data retention without any cause must always remain an exception and – especially in combination with other existing data collection – must not lead to the possibility of virtually reconstructing all the citizens' activities. The Federal Republic of Germany has to stand up for this purpose in the European and in the international context.

Information sources:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (judgment in German)

http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html (press release in German)
http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (press release in English)
During the period being reported on, there was a controversial discussion on German tax authorities acquiring tax data CDs originating from 'shady sources' abroad which contain information about alleged German tax evaders. Meanwhile, the Federal Constitutional Court has ruled that for further investigations relating to tax law the initial suspicion may be supported by data from a tax data CD acquired by German authorities. In the case that had to be decided by the Court, one informant from Lichtenstein had sold a CD-Rom containing information on suspected tax evaders to the Federal Intelligence Service who made this CD available to the tax authorities (see Federal Constitutional Court, Decision of 9 November 2010, 2BvR 2101 / 09).

## C. Other important information

### Handling geo-data in accordance with data protection requirements

In response to the ongoing discussions about the internet geo-data service Google Street View, the internet industry, under the leadership of the industry association BITKOM, presented in December 2010 a Data Protection Code which is intended to take the owners' and residents' interests into account when it comes to publishing views of buildings on the internet. The Code has been neither coordinated with the German data protection authorities, nor made adequate from a data protection perspective, because the self-commitment of the internet industry only provides for a right of objection after the publication of the views of buildings on the internet, and because the self-commitment is only binding for companies having signed the Code. However, the data protection authorities regard a right to objection before the publication as necessary, and also demanded that the Code not only include views from the street perspective, but also oblique aerial photographs. Therefore, the data protection authorities have called upon the legislator to take action.

### The new Act on Identity Cards

With the entry into force of the amended Act on Identity Cards on 1 November 2010, the new identity card was introduced in Germany. The new specific feature of this identity card is that it can be used, in addition to complying with statutory functions, as electronic proof of identity. It is equipped with a chip containing separated areas for biometric data and identification data stored for statutory purposes, for an electronic signature and for the electronic identity function (e-ID function). The use of the e-ID function and of the electronic signature function is voluntary, and it is also up to the ID holder to decide whether, in addition to the mandatory photograph, fingerprints must also be included.
From a data protection point of view, the positive aspect of the new identity card is in particular the possibility to use offers on the internet safely and pseudonymously by means of an identifier that is specific to services and cards.

### RFID (Radio Frequency Identification)

In order to examine threats to data protection when using RFID, a concept for assessing impacts on data protection – Privacy Impact Assessment (PIA) – was developed at the European level. The German industry was also involved in the development of the concept. In future, industry, the commerce sector and the business sector using RFID have to write reports and to submit them to the national supervisory authorities before commencing the operation. In April 2011 the PIA developed in this context was officially adopted by the European Commission.

Furthermore, the Federal Office for Security in Information Technology (BSI) published a new document containing basic principles on data security and data protection when it comes to using RFID. The document explains the complementary significance of the BSI's technical guidelines for the safe use of RFID and the European Commission's PIA framework.

# GREECE

## A. Summary of activities and news

In 2010, following a two-year effort, a progressive increase, within a three-year period, of the number of staff members by 25 (19 lawyers and IT experts and 6 administrative staff members) was approved by a decision of the Assistant Minister of Finance. Nevertheless, this increase is at risk of remaining on paper only because of the current public financial situation. Therefore, the HDPA remains unable to respond promptly to the numerous claims submitted by the citizens and the data controllers.

The only realistic solution for the HDPA to effectively operate under the current circumstances is to pursue two main objectives, preventive action and the selective handling of complaints and requests. As to the second objective, an amendment of the Data Protection Law (Article 19, paragraph1) has passed, allowing the HDPA to prioritise the cases to be handled on the basis of the criteria of the importance and the general interest of the issue.

As regards the first objective, the HDPA declared 2010 as the year of preventive action. The HDPA issued one guideline and drafted two more (issued early in 2011), delivered four opinions on new legislative proposals, issued pilot decisions for matters that data controllers from different sectors deal with and carried out ex-officio inspections in the IT systems of several main hospitals with the purpose of issuing related best practice guidelines in the near future.

More specifically, the HDPA gave advice to the Government via the following opinions and decisions: Opinion 1/2010 (on the publication of administrative acts containing personal data on the internet for the purpose of transparency), Opinion 2/2010 (on the use of CCTVs for the purpose of national security and the prevention and investigation of criminal offences), Opinion 4/2010 (on the e-card, for the electronic storage of purchase receipts for the purpose of taxation), Decision 43/2010 (on the census of state paid employees and the storage of the relevant information on a Governmental website), Decision 56/2010 (on the inclusion of the social security number – which reveals the date of birth – of doctors and pharmacists on prescriptions), etc.

The HDPA also issued the following opinion and pilot decision: Opinion 3/2010 (on the entry of aliens in the Schengen Information System and the National Record of Undesirable Aliens) and Decision 73/2010 (on the right of access of the defendant to the complainant's identification data when a complaint is submitted to a public authority). Finally, Guideline 1/2010 addresses the processing of personal data for the purpose of political communication.

On European Data Protection Day, the HDPA ran various activities. An Information Kiosk operated in front of the HDPA premises, in order for the Authority to raise awareness about data protection and its activities, familiarise citizens with the use of its website, distribute educational material and show various video clips including the Norwegian contribution from their 'You decide' campaign. Two informative leaflets were produced and distributed, one referring to the general principles of data protection and the other to unsolicited communications. A poster was also prepared for the event and aimed at drawing citizens' attention to situations where they are asked to give their personal data. Finally, the HDPA organised a press conference to present important current data protection issues, such as legal developments, social networking and street view services.

Finally, the Minister of Justice established a legislative Committee, following a request by the Hellenic Parliament, which shall examine the potential merger of independent authorities with related responsibilities and the improvement of their legal status, as provided by Law 3051/2002.

| Organisation | |
|---|---|
| Chair and/or College | Christos Yeraris (Chair) |
| Budget | EUR 2 923 500 |
| Staff | Auditors Department: 16 lawyers and 11 IT experts (of whom 7 are on maternity leave, and 2 were for part of the year seconded to European bodies as national experts);<br>Communications and Public Relations Department: 6 (of whom 1 resigned, 1 was on secondment, 1 was on secondment for half of the year and 1 was on maternity leave for half of the year);<br>Human Resources and Finance Department: 17 (of whom 1 was on maternity leave) and 1 seconded from another civil service. |
| General Activity | |
| Decisions, opinions, recommendations | The HDPA issued 11 decisions, 4 opinions and 1 guideline, which have an effect on data protection in general. |
| Notifications | The HDPA examined 759 notifications (430 of them concerned the installation and operation of CCTVs and 73 data transfers to countries outside the EU). |
| Prior checks | The HDPA granted or renewed 63 permits concerning the processing of sensitive data, interconnection of files and data transfer to countries outside the EU). |
| Requests from data subjects | 1 507 (data subjects and data controllers) |
| Complaints from data subjects | 674 (Prosecution Authorities and Public Order: 8, National Defence: 1, Public Administration and Local Government: 32, Taxation – Ministry of Finance: 6, Health: 17, Social Security: 31, Education and Research: 12, Banking: 45, Private Economy: 208, e-communications: 97, Work Relations: 45, Mass Media: 9) |
| Advice requested by parliament or government | 7 (Opinion 1/2010, Opinion 2/2010, Opinion 3/2010, Opinion 4/2010, Decision 43/2010, Decision 56/2010, Decision 19/2010) |
| Other relevant general activity information | |
| Inspection Activities | |
| Inspections, investigations | 11 inspections in the health care sector, 1 in a social security fund/organisation |
| Sanction Activities | |
| Sanctions | 8 sanctions (1 warning, 7 penalties) decided by the DPA in the following sectors: health care (1), insurance (2), bank (1), private economy (2), mass |

| | |
|---|---|
| | media (2) |
| Penalties | Amounts: EUR 1 000 – EUR 10 000 (total EUR 29 500) imposed by the HDPA |
| DPOs | N/A |
| Figures on DPOs | N/A |

## B. Information on case-law

### Guideline 1/2010

The HDPA defined the rules for the lawful processing of personal data for the purpose of political communication. It provided guidance as to the lawful sources for collecting data and the means (post/electronic) used for political communication.

### Opinion 1/2010

The HDPA delivered an opinion on a draft bill concerning the compulsory publication of administrative acts containing personal data on the internet. The Authority asked for a time limitation regarding the publication on the internet of such acts and technical measures in order to prevent the use of such data for other purposes. Finally, it considered that acts containing sensitive data must not be uploaded.

### Opinion 2/2010

The HDPA, following its Opinion 1/2009, formulated certain proposals for the operation of CCTV systems in public places for the purpose of national security, the prevention and investigation of criminal offences and the monitoring of traffic. The HDPA's proposals were mainly adopted in Article 14 of Law 3917/2011. A Presidential Decree shall further specify the criteria and the safeguards for the operation of CCTV systems for the aforementioned purposes. The HDPA is involved in the drafting of this Decree. Meanwhile, in early 2011, the HDPA issued Guideline 1/2011 for the operation of CCTV systems for the purpose of protection of persons and goods.

### Opinion 3/2010

The HDPA receives numerous complaints every year from aliens requesting to be deleted from the Schengen Information System (SIS) and the National Record of Undesirable Aliens (NRUA) on the basis of Article 96 of the Convention implementing the Schengen Agreement. For this reason the HDPA after having exchanged views with the Ministry of Citizen Protection issued Opinion 3/2010.

### Opinion 4/2010

An opinion was delivered on the set-up of an optional system for registering taxpayers' purchase receipts with the purpose of releasing the taxpayers from the burden of keeping the receipts for tax reasons, at the same time checking the tax compliance of companies. It is based on a new magnetic card utilising the existing Point of Sale terminals for transactions via debit and credit cards. The HDPA asked for a clear legal basis for such processing, which will provide for the optional use of the system by taxpayers and the details of the processing in order to ensure the foreseeability of the law. Moreover, it highlighted the need for adequate security measures, so that banks, acting as data processors, will not be able to use the data for their own purposes.

### Decision 7/2010

The HDPA rejected a request by the Greek Car Rental Companies Association to create a blacklist of insolvent clients, as a) the financial risk is not so critical as to threaten this particular business sector, b) the financial damage, which small enterprises suffer because of the theft of uninsured vehicles, is their own business choice, and c) the Association had not considered whether the same purpose could be pursued by less privacy-intrusive means.

### Decision 8/2010

The HDPA judged that the publication of sensitive data related to a criminal prosecution in the electronic edition of a newspaper was unlawful because the claimant was not a public figure. The HDPA imposed a fine on the controller and prohibited the further publication of the disputed article in the printed edition of the newspaper. It also ordered that the article already uploaded be anonymous, and recommended measures to avoid future violations.

### Decision 31/2010

The HDPA examined a biometric access control system in specific critical infrastructures of the 'Macedonia' International Airport in Thessaloniki, which was planned to be set up within a research project. This project aims at developing a privacy-friendly biometric method based on fingerprints. The HDPA ruled that the system was in line with Law 2472/1997, subject to the following conditions: the data controller must develop a security policy for the data processing and notify the HDPA of the deletion of the data after a one-year period, which is required for accomplishing the processing purpose. The retention of the raw biometric data in a central database was forbidden.

### Decision 43/2010

The HDPA examined, both ex officio and in response to complaints, the census process of state paid employees, which was introduced in July 2010 following a Ministerial Decree. The HDPA ruled that this legal basis allows processing only for payroll purposes, and decided that any other data, not necessary for these purposes, shall not be processed. As for the security measures, the HDPA asked for concrete measures relating to the authentication process and the protection of the data against unauthorised access.

### Decision 56/2010

The HDPA concluded that the legal provision aiming at the control of public health expenses, and to this end imposing the inclusion of doctors' and pharmacists' Social Security Numbers (SSN) on every prescription for the purpose of unique identification, complied with the constitutional principle of proportionality. Even though the date of birth is part of the SSN, it does not seriously affect doctors' and pharmacists' privacy, since the age is only revealed to a limited number of users under specific circumstances, as clearly provided for in the law. However, the HDPA recommended that the State should design the SSN in a way that does not directly reveal personal data.

### Decision 73/2010

The HDPA deemed that the defendant has the right to have access not only to the content of the complaint itself, lodged with a public authority, but also to every detail concerning the source of these data, including the complainant's identification data. This right may be limited if access would put at risk the investigation conducted by the authority, if the document contains information subject to specific secrecy obligations or about the private or family life of a third person or if the disclosure may put the complainant's life at risk. The complainant must be adequately informed at the time of the submission of the complaint and asked to justify in writing his or her objections against the disclosure.

## HUNGARY

### A. Summary of activities and news

In the course of the procedure of reviewing the Constitution, the proposals of the Data Protection Commissioner were sent to the Ad hoc Committee responsible for the preparation of the new Basic Law. According to the view of the Commissioner: (1) instead of a data protection commissioner, the appointment of an information commissioner would be preferable; sustainable regulation as an effective solution should involve entrusting the data protection supervisory body with the supervision of freedom of information related regulations, (2) through the amendment of the regulations, the independence of the institution should be strengthened, and (3) an information commissioner responsible for two kinds of information rights should have effective tools for enforcement.

Awareness-raising activities carried out by the Data Protection Commissioner followed the path of successful practices of former years and many information events were organised. The data protection conference organised on Data Protection Day was devoted to the analysis of problematic issues of surveillance systems, developments of surveillance technologies, how legislation responds to these developments, whether these systems are effective tools in law enforcement, what the actual benefits identified for society may be, and whether these systems may be treated as a proportionate means, considering the purpose foreseen.

The international conference organised on 28 September aimed at finding a balance between data protection and freedom of information.

The development of a publication was started in 2009 with the Polish and the Czech DPAs. This publication concentrated on data protection issues related to employment/entrepreneurs operating in these three countries. The publication containing relevant EU and national legislation, national best practices and recommendations was scheduled to be published in 2011.

| Organisation | |
|---|---|
| Chair and/or College | Mr András Jóri Ph.D.<br>Parliamentary Commissioner for Data Protection and Freedom of Information. |
| Budget | HUF 374 109 000 |
| Staff | 48 |
| General Activity | |
| Decisions, opinions, recommendations, | No collected statistics are available. |
| Notifications | 15 161 |
| Prior checks | N/A |
| Requests from data subjects | These two categories together: 2 013 |
| Complaints from data subjects | |
| Advice requested by parliament or government | 639 |

| | |
|---|---|
| Other relevant general activity information | Consultations: 1 035 |
| Inspection Activities | |
| Inspections, investigations | No collected statistics are available. |
| **Sanction Activities** | |
| Sanctions | N/A |
| Penalties | N/A |
| **DPOs** | |
| Figures on DPOs | N/A |

## B. Information on case-law

The Data Protection Commissioner initiated several projects in a proactive manner that responded to the most relevant issues, with all of them complying with Directive 95/46/EC as well.

A comprehensive research project was completed, ending with a recommendation focusing on data processing in the press and media. It reviewed the regulations and practice, and identified areas for the protection of privacy and personal data in the press/media, in particular covering: the analysis of the interrelation of personal rights protecting personal data and privacy; the personal data content of information appearing in the media, the source of data, legal authorisation, the obligation to inform data subjects and the requirement of purpose limitation; practice regarding the consent given in the course of appearances in the media, complaints, law reform; effects of regulations on investigative journalism on data protection regulations; and regulation of criminal journalism.

The project on surveillance by cameras analysed the social effects, advantages and disadvantages of operating such systems. The aim was to establish clear and practical solutions and arguments that can be effectively used in discussions. Surveillance by cameras does not fit into the legal environment and compliance with the law is often poor, which is detrimental to data protection. The purpose was to update the former recommendation on this issue.

Due to the intensified efforts of the legislator to set up a thorough credit reference system based on business grounds, in connection with which the Commissioner published several positions since he did not see adequate safeguards related to the voluntary nature of the consent of debtors, a project was started to explore how guarantees may be complied with.

Representatives of Google initiated discussions in the office about data protection requirements necessary for the launching of the Google Street View service in Hungary. In the course of the investigation the Commissioner asked Google to suspend the taking of photos until the legal basis was clarified. It was already stated in advance that, according to the data protection act and the act on the civil code, the taking of photos of public places is not illegal. Clear requirements had to be specified before the activity of Google could be started. The discussions and the preliminary position of the Commissioner took into consideration the European views in this respect. The final decision will be issued based on the replies of Google to questions of the Commissioner and results of the investigation in 2011.

The use of widely available modern technologies saw the Commissioner investigate many areas. In the field of employment the tendencies remain typical, camera surveillance systems are operated, geolocalisation, polygraphs and other means are often applied by employers, mail boxes are checked, and even medical tests are required by employers. Given this constant state, the huge number of complaints showed that the field of employment had become a sector that needed a more comprehensive, concept-based and detailed regulation.

The field of education proved to be invading privacy as well. Educational institutions set up enrolment systems utilising easy access technologies which were not appropriately applied. Surveillance cameras and biometric identification were the most prevalent examples in relation to which the Commissioner found that proportionality and purpose limitation was not being complied with by the institutions. In a case concerning international exams, candidates, in addition to providing personal identification documents, were required to provide fingerprints and have their signatures digitalised before they could sit the exam. Failure to provide this information would have resulted in exclusion from the exam. In the latter case, the principle issue in dispute was the voluntary, 'freely given' nature of the consent.

Finally, there was a case in the field of telecommunications, in which photos and identifying data (very often name, telephone number, etc.) were uploaded to a social networking site, together with obscene statements and references about the complainant. Since clearly personal data were concerned, the processing of such information could only be lawful if there was consent from the data subject. In this case, consent was deemed to be missing, so the Commissioner laid a complaint with the police (i.e. offence of misuse of personal data). An investigation was begun by the police; however, the whole content was deleted from the Hungarian portal and uploaded to other file-sharing sites in countries beyond the jurisdiction.

## IRELAND

### A. Summary of activities and news

The Office of the Data Protection Commissioner opened 783 formal complaints for investigation in 2010 (many complaints are dealt with informally by providing the complainant with appropriate information on their rights). As in previous years, the vast majority of complaints were resolved amicably, with only 14 complaints giving rise to formal decisions. Information in regard to prosecutions in 2010 is included in Section B of this report. There was a large increase in personal data security breach notifications to the Office, mainly as a result of the introduction in July 2010 of a new Personal Data Security Breach Code of Practice. The Commissioner continued to engage with large public sector organisations about the extent of data sharing in the public sector. On the basis of these engagements and a number of audits of organisations in the sector, the Commissioner has agreed a set of guidelines for all public sector organisations, with transparency and proportionality as guiding principles. Other guidance issued included revised personal data security breach guidance, revised data security guidance and new employee vetting guidance.

| | |
|---|---|
| **Organisation** | Office of the Data Protection Commissioner |
| Chair and/or College | Billy Hawkes |
| Budget | EUR 1 272 000 (EUR 1 449 329 spent) |
| Staff | 22 |
| **General Activity** | |
| Decisions, opinions, recommendations | 3 (Guidance) |
| Notifications | There were approximately 5 000 registrations in 2010. |
| Prior checks | N/A |
| Requests from data subjects | 7 200 |
| Complaints from data subjects | 783 (access rights – 39%, electronic direct marketing – 30%, disclosure – 10%, unfair processing – 10%, other – 11%) |
| Advice requested by parliament or government | 54 |
| Other relevant general activity information | 410 personal data security breach notifications from 123 different organisations |
| **Inspection Activities** | |
| Inspections, investigations | 32 audits (inspections) |
| **Sanction Activities** | |
| Sanctions | 8 companies and individuals were prosecuted in 2010. |

| | |
|---|---|
| Penalties | EUR 11 050 + costs (fines/settlements imposed by courts) |
| DPOs | |
| Figures on DPOs | N/A |

### B. Information on case-law

In most cases, in accordance with Section 10 of the Irish Data Protection Acts 1988 and 2003, complaints submitted to the Commissioner are resolved amicably without resorting to a formal decision or enforcement action. Such amicable resolutions may, for example, involve a financial contribution by the relevant data controller to the data subject concerned or to an appropriate charity. Where necessary, enforcement powers are used – for example, when data controllers fail to respect the access rights of data subjects. In some cases, data controllers are named in case studies included in the Commissioner's Annual Report. In the course of 2010, the Commissioner engaged in several successful prosecutions related to the rights of data subjects under the Data Protection Acts 1988 and 2003 and under Statutory Instrument 535 of 2003 (implementing Directive 2002/58/EC in Ireland). Seven companies were prosecuted for various offences in 2010 and, for the first time, the Office prosecuted two individuals (resulting in a criminal record for one individual). This prosecution related to unsolicited marketing text messages.

### C. Other important information

Also in 2010, the Commissioner conducted a comprehensive investigation of a claims database shared by the insurance sector, known as Insurance Link. At the time of the investigation, the database contained details of almost 2.5 million claims. The resulting report described a lack of transparency, inadequate access controls and patterns of inappropriate access.

## ITALY

### A. Summary of activities and news

The main areas of activity for the Garante in the course of 2010 were the following:

- health care (electronic health record and health file, online examination records, booking and collection of examination records in pharmacies, scientific and pharmacological research, project of epidemiologic surveillance on soldiers in Bosnia, collection of HIV data in health care institutions, privacy rights in hospitals/health care institutions, storage of medical documents);
- public administration (dissemination of data on real estate owned by public entities, transparency of grants and salaries accorded by public administrations, online publication and dissemination of personal data by public bodies, data base on paedophilia, registry for homeless persons, security measures for the *Anagrafe tributaria* [i.e., the information system of the Revenue Service], interconnection and security of public data bases);
- marketing (unsolicited phone calls and opt-out register [*Registro delle opposizioni*], spam, fax and unsolicited e-mails);
- electronic communications (smartphones and tablets, storage of telephone and internet data for judicial purposes, 'reverse searches', security measures, customer profiling);
- journalism and information (judiciary records reported by the press, protection of the privacy rights of children and victims of violence, data on health and sexual activity, adoption, pictures of persons under arrest, newspaper archives on line);
- employment (detection systems based on biometric data, employee location systems, monitoring employees' use of the internet, video surveillance in the workplace);
- police and justice (judicial data as related to mediation activities aimed at conciliation of civil and commercial disputes; digital civil trial [e-justice], security measures for judicial offices, new information system for the administrative justice, CED – IT database of the Police Public Security department, air passengers' data, security measures for the Schengen database);
- internet (search engines, Google Street View, Google Buzz, Facebook and social networks, unlawful storage of internet usage data, forums and blogs, simplified security measures for small internet service providers, online profiling);
- new technologies (geo-location, RFID-based technologies);
- schools and universities (*anagrafe nazionale degli studenti* [national students' registry], use of video surveillance in schools, publication of grades and exam results, pupils' rankings, personal data used for enrolment with universities);
- private bodies (*tessera del tifoso* [soccer fan card], wedding agencies, ski pass, condos);
- corporations (transfer of data to third countries, data relating to social security, rating agencies and monitoring of conflicts of interest, simplified data protection measures, information of a commercial nature);
- banks, financial institutions and insurance companies (access to clients' data held by banks, security measures, information systems on credit histories, access to consumer credit data by EU lenders).

The DPA was heard several times as part of **Parliamentary Hearings** on major issues involving, in particular, immigration policy, *anagrafe tributaria*, and simplification of the relationship between the public administration and citizens.

The Garante also approved important **guidelines** concerning, in particular, disclosure of information on legal persons; the rules to be complied with by public administrative bodies when posting administrative records and documents

that contain personal data ('public administration on the internet'); and customer satisfaction measurement in the health care sector.

The Garante provided **general decisions** on specific sectors: video surveillance; electoral propaganda; *tessera del tifoso* (soccer fan card); telemarketing; number portability; credit information systems; telephone registries and 'reverse searches' (i.e. the ability to retrieve user-related data via the user's telephone number); use of the data in the *pubblico registro automobilistico* (i.e. the registry containing data relating to vehicles); and security measures for customer data held by banks.

Concerning international relations and the cooperation of the Garante with other DPAs, besides the work done in the context of the Article 29 Working Party and its thematic sub-groups (where the Garante acted as rapporteur for the joint enforcement action on the application of the Data Retention Directive 2006/24/EC), the Garante actively participates in the working groups on data protection at the OECD (Working Party on Information Security and Privacy – WPISP) and at the Council of Europe (T-PD consultative committee of Convention 108/1981 and T-PD Bureau, of which the Garante is a member).

The Italian DPA is also a member of the Joint Supervisory Authorities and of other multiparty oversight bodies based on legal instruments of the European Union that have set up common information systems (JSB Europol, Schengen, Customs, Eurodac).

The DPA takes part in the meetings of the International Working Group on Data Protection in Telecommunications (IWGDPT) and in the meetings of the Case Handling Workshop, established at the Spring Conference of the European data protection authorities.

In the field of judiciary and police cooperation, the Italian DPA carried out its work on promotion and enforcement of data protection in the context of the WPPJ (Working Party on Police and Justice), chaired by the President of the Garante, Prof. Pizzetti.

As usual, the DPA was directly involved in both the European and the International Conference held this year.

The Garante, in line with its previous actions, also focused its attention on awareness-raising initiatives, especially aimed at young people, in particular by issuing booklets on social networks, school, and the health sector. In line with this objective, the Italian DPA launched a competition for high school students called 'Privacy 2.0. Youths and New Technologies'.

The Garante is required by law to submit an annual report to Parliament on the work done. The Annual Report for the year 2010 was accompanied by two information documents – on cloud computing and on smartphone and tablets – which lay out common principles and guidance on data protection as adapted to the new technological developments partly based on the experience and expertise of the DPA (see paragraph C).

| Organisation | *Garante per la protezione dei dati personali* |
|---|---|
| Chair and/or College | Chair: Prof. Francesco Pizzetti<br>College: Giuseppe Chiaravalloti<br>Mauro Paissan<br>Giuseppe Fortunato |
| Budget | Approximately EUR 16.5 million |
| Staff | 118 |
| General Activity | |
| Decisions, opinions, recommendations | Number of decisions taken by the College: approximately 600 |
| Notifications | 1 197 |
| Prior checks | Approximately 10 |
| Requests from data subjects | Total number of requests: approximately 4 000<br>Requests for information (*quesiti*): 353<br>Reports and claims (*segnalazioni* and *reclami* received in 2010) from data subjects: 3 359 |
| Complaints from data subjects | (Formal complaints, specifically regulated by the DP Code, concerning access to one's personal data) Approximately 350 |
| Advice requested by parliament or government | Opinions in reply to Parliamentary inquiries: 4<br>Opinions to Ministries and to the PM's Office: 16<br>Topics: police, public security: 4<br>Judicial activity: 1<br>E-government and databases: 5<br>Education and training: 2<br>Employment in public bodies: 1<br>Health care: 1<br>Businesses: 1 |

| | |
|---|---|
| | Welfare: 1<br>Marketing (by means of telephone calls): 1 |
| Other relevant general activity information | The front office of the DPA received, in 2010, over 26 000 telephone calls and emails; they mostly concerned telemarketing, e-mail and fax spamming, video surveillance, internet and social networks, and the protection of privacy in the workplace (both public and private sector).<br><br>National authorisations for BCR: 2 |
| Inspection Activities | |
| Inspections, investigations | Number of inspections and/or investigations (on the spot):<br>approximately 500 (in 55 of which infringements having a criminal nature were reported to the judicial authority).<br>Key topics: missing information notice; lack of security measures; failure to provide information and/or documents to the Garante; missing or incomplete notification to the Garante; breach of a decision by the Garante; breach of provisions on data retention; multiple breaches by data controllers of large-scale or sensitive data databases. |
| Sanction Activities | |
| Sanctions | Approximately 500 |
| Penalties | Amount: approximately EUR 4.8 million imposed by financial police in charge of controls on the DPA's behalf. |
| DPOs | |
| Figures on DPOs | N/A (no DPOs are provided for in the Italian legal system) |

## B. Information on case-law

The **Court of Milan** found the managers of Google in breach of Section 167 (unlawful data processing, including the dissemination of sensitive data) of the Privacy Code [Legislative Decree No 196 dated 30 June 2003]. The breach consisted of the dissemination on a website of a video showing a disabled minor harassed by his schoolmates (Decision of 24 February 2010).

The **Court of Palermo** ruled that a bank was liable vis-à-vis two customers for carrying out a non-authorised bank transfer to a third country via its online banking service, which was not adequately protected by security measures. The decision is based in particular on Section 15 of the Privacy Code, laying down that whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages pursuant to Section 2050 of the Civil Code [liability stemming from the exercise of activities having a dangerous nature] (Decision of 20 December 2009).

The **Council of State (highest instance administrative court)** ruled that the data subjects' right to have their data rectified, according to Section 7 of the Privacy Code, must always be ensured in order to uphold accuracy of the personal data held in the *casellario giudiziale* (i.e. the registry containing judicial records), (Decision No 473/2010).

The **Council of State** endorsed a request – aimed at the annulment of marriage – to access administrative records disclosing sensitive data on the spouse's health. In fact, the remedy sought in the case (i.e. the annulment) represented a legal claim that was not overridden by the data subjects' right to privacy. Therefore, according to Section 60 of the Privacy Code, the Supreme Court of Administrative Justice upheld the request for disclosure of sensitive health data (Decision No 7166/2010).

The **Court of Cassation** ruled that the dismissal of an employee, based on the fact that the latter had been found to be surfing on the internet on several occasions for personal purposes, had to be considered unlawful. In fact, the finding in question had been made by means of software – deployed by the employer – allowing access to the data contained in the personal computers used by his employees. Pursuant to Act No 300/1970 ('Workers' Statute' – *statuto dei lavoratori*), the Court expressly affirmed that: 'the control of the employees' activity', though necessary, 'has to be kept within the boundaries of a 'human dimension' and it shall not be exacerbated by the recourse to technologies that entail the violation of all forms of privacy and autonomy in the discharge of the work duties'. IT devices 'that allow monitoring internet 'navigation' are 'equipment intended for distance monitoring' of the employees.' Therefore, the deployment of such systems 'is subject to an agreement with the trade union's representatives in the office or, in the absence of such agreement, to the authorisation of the Labour Inspectorate (Section 4.2 of the Workers' Statute).' Data obtained in breach of this provision cannot be used before the judicial authority (Decision No 4375/2010).

The **Court of Cassation** – in a case also addressing the same issue of legitimacy of an employee's dismissal – ruled that respect for the right to privacy cannot *per se* prevent the exercise of other fundamental rights, such as the right to defence or the right to work. In such cases, it becomes of paramount importance to strike the right balance between the different rights at stake (Decision No 18279/2010).

### C. Other important information

The DPA started a survey on the main producers of **smartphone** software systems in order to verify the adequacy of the security measures in relation to the mobile apps developed for such systems. The replies received so far have shown that the adopted security policies diverge in many respects. The main critical aspects highlighted by this survey were described in a document called 'Smartphones and tablets: Current scenario and operational perspectives' which was annexed to the annual activity report of the Garante in 2010.

Via a booklet called *Cloud computing: guidelines for a knowledgeable use of these services*, the Garante provided initial guidance for the users of cloud computing services (e.g.: need for prior risk-based assessment, also including reliability of the individual provider; and a check of the specific contractual clauses including the location of the cloud server, the typology of services offered, and training of the personnel in charge of data processing) in order to foster the mindful use of such services and with a view to providing specific rules on security measures in the near future.

**Video surveillance**: this issue was recently addressed by a **general decision** of 27 April 2010, which is binding on both public and private entities with respect to the installation of CCTV and video surveillance systems. The rules set out in this general decision provide specific safeguards for the privacy of the individuals whose data are collected and processed via such systems. This replaces a previous decision issued by the DPA in 2004 to take account not only of the supervening legislation, but also of the new technologies and the substantial increase in the use of video surveillance for multifarious purposes. Special attention was given to measures informing data subjects that CCTV cameras are in operation in the areas/premises they are about to access (obligation to provide specific information notices, except in the case of CCTV cameras in use for public security purposes) and to the limits on retention of data collected by CCTV cameras and video surveillance systems (the images, where recorded, should be kept for a limited period of time, which should not be in excess of 24 hours. A longer retention period is envisaged in specific cases, such as police and judiciary investigations, security of banks, etc.).

## LATVIA

### A. Summary of activities and news

The 2010 amendments to the Personal Data Protection Law were adopted by the Parliament of the Republic of Latvia on 6 May 2011 (in force since 2 June 2010). Namely Article 10, Chapter 4 of the Personal Data Protection Law was amended, thus determining the exceptions where personal data processing is allowed for purposes other than those initially foreseen within criminal law cases. Another important amendment is related to the decisions of the Data State Inspectorate (Article 31, Chapter 2) – challenging or appealing against the administrative acts issued by the Data State Inspectorate regarding the blocking of personal data processing, as well as regarding permanent or temporary prohibition of personal data processing, does not suspend the implementation of the Data State Inspectorate's decision (unless suspended with the decision of the appeal's reviewer).

At the national level, the Data State Inspectorate of Latvia provided its opinion regarding various legal acts and policy initiatives. The main ones are as follows:

- Draft Law on the Credit Register – the opinion was provided to the National Bank of Latvia regarding data subjects' right of access to this register, as at the beginning there was a restriction to these rights that does not comply with the Personal Data Protection Law; the opinion of the Data State Inspectorate was taken into account.
- Draft Law on Debt Retrieval – pursuant to an opinion of the Data State Inspectorate, it was determined that personal information cannot be included in a credit reference data base if the person has objected to the existence of the debt.
- Draft Law on the amendments to the Consumer Rights Protection Law – the opinion of the Data State Inspectorate was taken into account where it was indicated that these draft amendments did not take into account the application restrictions of EC Directive 2008/48/EC regarding the amount of credit and the conditions under which it is not necessary to check the creditworthiness of a customer.
- The Data State Inspectorate of Latvia has not been taking part in projects at the national level to introduce the e-health policy. However, in 2010, the Data State Inspectorate carried out an inspection regarding sensitive personal data processing within the health sector. The investigations were to be continued in 2011.

#### Key topics where advice was requested by public authorities

The Data State Inspectorate does not have statistics on the requests for advice submitted by public authorities. However, the Data State Inspectorate receives daily calls from different public authorities on a variety of issues related to personal data processing – for example, the need to notify about personal data processing, and more complicated questions requiring in-depth analysis to find the best solution regarding personal data protection.

#### Information on awareness-raising activity

The Data State Inspectorate has organised several seminars on the issues for personal data protection, for different target audiences – for instance, directors of educational establishments, teachers, etc. The Data State Inspectorate provides seminars which are open to all persons interested (three such seminars organised in 2010).

| | |
|---|---|
| Organisation | Data State Inspectorate of Latvia (*Datu valsts inspekcija*) |

| | |
|---|---|
| Chair and/or College | Director – Signe Plūmiņa |
| Budget | LVL 266 907 (approximately EUR 370 457) |
| Staff | 19 (including administrative and maintenance staff) |
| General Activity | |
| Decisions, opinions, recommendations | Regarding the statistics on decisions, opinions – N/A.<br>Regarding the recommendation – the recommendation was shown on social networks (targeted at users of social networks). |
| Notifications | 352 (including the notifications on amendments to personal data processing) |
| Prior checks | 267 |
| Requests from data subjects | N/A |
| Complaints from data subjects | 234 complaints from data subjects regarding a possible personal data protection breach.<br>2 complaints from data subjects from third countries regarding their personal data processing within SIS.<br>22 complaints regarding SPAM (15 investigations carried out). |
| Advice requested by parliament or government | 9 (regarding amendments to the Personal Data Protection Law and the draft of the Information Technology Security Law) |
| Other relevant general activity information | In telephone consultations, the main questions asked by the callers were:<br>• Is certain information considered as personal data?<br>• Who can carry out video surveillance, and when and where?<br>• How can one fight against unlawful personal data processing on the internet?<br>• What about personal data processing within the debt-collection process?<br>• When is one allowed to process personal codes and who is allowed to do this? |
| Inspection Activities | |
| Inspections, investigations | 234 complaints:<br>Most people who contacted the Data State Inspectorate of Latvia indicated a possible breach of the Personal Data Protection Law in the following areas:<br>• personal data processing on the internet (also in cases when the controller has not foreseen appropriate technical means for data protection);<br>• personal data processing related to debt collection and setting up |

| | |
|---|---|
| | the credit history;<br>• identity theft – when personal data of another person are provided, thus unlawful personal data processing is carried out (many cases regarding wrong personal data submitted to State or Local Government Police regarding several administrative violations);<br>• data processing carried out by house maintenance companies;<br>• video surveillance. |
| Sanction Activities | |
| Sanctions | The power of the Data State Inspectorate to impose sanctions is provided for in the Latvian Administrative Violations Code. The breach of Personal Data Protection Law was concluded in 42 cases, and administrative fines were imposed.<br>Not all the investigations initiated were accomplished in 2010. |
| Penalties | Amounts (indication of whether imposed by courts or DPAs).<br>Amounts imposed by the Data State Inspectorate – 28 warnings; 14 fines – the total amount of fines was LVL 14 250 (approximately EUR 19 249). |
| DPOs | |
| Figures on DPOs | 9 data protection officers registered.<br>4 exams for data protection officers organised. |

## B. Information on case-law

In 2010 the number of cases where the Personal Data Protection Law had been violated increased. The sanctions for such violations are provided for in criminal law. Thus, these cases were forwarded to the office of the prosecutor general.

The Data State Inspectorate has concluded that there is a need for better cooperation on the EU level in order to fight against data protection breaches on the internet more effectively, thus ensuring the rights of EU citizens to protection of their data.

## LITHUANIA

### A. Summary of activities and news

The Law amending and supplementing the Law on Legal Protection of Personal Data (Official Gazette, 1996, No 63-1479; 2008, No 22-804) was adopted on 12 May 2011 and will come into force on 1 September 2011. The new wording of the Law on Legal Protection of Personal Data (hereinafter – LLPPD) states that, in terms of accepting risk and creditworthiness, financial institutions that provide financial services may disclose to each other the personal data on marital status, current job position and education, for the purpose of financial risk assessment and debt management of data subjects to whom these financial institutions have rendered or intend to render financial services, on the condition that the data subjects concerned have given their consent. Also, the new wording states that when carrying out social and public surveys, personal data may be processed if the data subject has given his or her consent.

The Law on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters implementing Council Framework Decision 2008/977/JHA was adopted on 21 April 2011 and was scheduled to come into force on 1 July 2011.

On 27 November 2010 a new version of the Law of the Government of the Republic of Lithuania came into force. New wording specifies changes to the legal status of the Director of the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI). The new version states that the Director of the SDPI will become a state officer. According to the new version of this Law, the SDPI shall operate according to the strategic plan approved by the Minister of Justice. Also, this law states that the Minister of Justice shall offer the Government the opportunity to appoint or to dismiss the Director of the SDPI, to promote him and impose penalties on him. Furthermore, the Minister of Justice decides the Director's holidays, and can send him on missions. According to this law, the Director of the SDPI is responsible and accountable to the Government and the Minister of Justice.

On 23 December 2009 the Government of the Republic of Lithuania adopted a Resolution on Council Decision 2009/371/JHA on the establishment of the European Police Office (Europol). According to Article 3 of this Resolution, the SDPI was appointed as the supervisory authority to carry out the implementation tasks of Article 33 of Council Decision 2009/371/JHA (entered into force on 1 January 2010).

European Data Protection Day was celebrated on 28 January 2010. A meeting in the European Information Office of the Seimas was organised. This event was devoted to the various state institutions, agencies and organisations whose activities are related to the protection of personal data. Representatives from the public sector were informed about current issues of personal data protection in Lithuania and other countries. Much attention was paid to video surveillance. Three reports on this topic were presented: 'Legal regulation of video surveillance', 'Technical video surveillance issues' and 'Video surveillance issues in the capital Vilnius – present and past'.

The SDPI together with the company Expozona held a conference entitled 'Data protection in the newest technologies and e-space' on 26 May 2010. The event focused on identity management, privacy and data protection in information and communication technologies, and mobility. These topics covered the main themes that were analysed during the four PrivacyOS (Privacy Open Space) project conferences. PrivacyOS brings together industry, SMEs, government, academia and civil society to foster the development and deployment of privacy infrastructures for Europe. The conference was attended by over 60 public and private sector representatives.

The SDPI together with the company Expozona also held a conference entitled 'Is personal data processed lawfully in Lithuania? Problems, causes and ways to solve them' on 24 November 2010. This event was targeted at directors of companies, institutions and organisations, lawyers and professionals who are responsible for the processing of employee and customer personal data. The speakers from the SDPI and from the law firm LAWIN Lideika, Petrauskas, Valiūnas and partners gave six presentations on different topics: 'What do you need to know in order to lawfully process personal data?'; 'The processing of employees' personal data. Problems and ways to solve them'; 'Complaint examination practice. Important court decisions on data protection'; 'Lawful transfer of personal data to data recipients in foreign countries'; 'The processing of special categories of personal data. Lithuanian and European Union practice'; and 'Current issues of personal data protection in Lithuania and Europe'.

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | Dr Algirdas Kunčinas |
| Budget | Allocated and executed LTL 1 886 million |
| Staff | 30 |
| **General Activity** | |
| Decisions, opinions, recommendations | Recommendation on 'Implementation of an individual's right to private life and data protection principles regarding applicable radio frequency identification means' |
| Notifications | 760 (about data processing) |
| Prior checks | 204 |
| Requests from data subjects | 8 |
| Complaints from data subjects | 270 |
| Advice requested by parliament or government | 1 |
| Other relevant general activity information | 3 294 consultations; 102 public information releases; 7 summaries of the results of the complaints investigation and case-law; 6 requests relating to data processing in the C.SIS; 86 conclusions on the EU and Council of Europe documents; 92 responses to enquiries from parties to the Convention (ETS No. 108); 238 coordinated legal acts and data controller documents; 5 prepared legal acts |
| **Inspection Activities** | |
| Inspections, investigations | 80 (data processing legitimacy and scope of registered users in social networking sites; legitimacy of data processing when providing fast credit services; legitimacy of storage of internet traffic data when providing internet services; scope and legitimacy of publishing personal data on municipalities' web pages; legitimacy of processing client personal data in privately owned sports clubs) |
| **Sanction Activities** | |
| Sanctions | The SDPI drew up 41 protocols of administrative violations (in 2010 only 29 protocol decisions by the court were issued). |
| Penalties | 23 |
| **DPOs** | |
| Figures on DPOs | N/A |

## B. Information on case-law

### Video surveillance in a beauty salon

The SDPI received a complaint in which it was stated that a beauty salon had installed video surveillance cameras and one of them was hidden and oriented so as to video-survey the whole body of the client; another was installed in the workers' locker room. The SDPI determined that such video surveillance was used without a written data controller's document regulating such surveillance, and was used in premises where the data subject reasonably expected absolute protection of privacy. The SDPI also found that the data controller did not provide any contact information to the data subject, did not notify the personnel in writing about the video surveillance and did not notify the SDPI about data processing by automatic means. For the breaches of the LLPPD, the SDPI drew up a record of administrative offences committed by the owner of the beauty salon. Vilnius City first district court accepted the record of administrative offences and issued a fine to the owner of the beauty salon.

### Lawyer's right to collect sensitive personal data

The SDPI received a complaint that a director of a hospital, pursuant to a lawyer's request based on a contract of legal representation with his client, gave permission to disclose to the lawyer the complainant's full personal health history, thus, possibly illegally, making public such history.

After an investigation it was established that the lawyer, on the basis of his legal representation contract and Article 44 of the Law of the Bar of the Republic of Lithuania requested the hospital to provide a transcript of the complainant's health history. The transcript was intended as evidence in court in order to establish if the fright from a dog attack, during which there was no physical contact between the complainant and the dog, had any effect on the complainant's health and if so, to what extent. The request was met and the lawyer presented the health history to the court.

Article 180 of the Code of Civil Procedure of the Republic of Lithuania states that a court shall only accept given information if it proves or disproves circumstances which are relevant to the case.

According to the LLPPD and Code of Civil Procedure, the SDPI concluded that full presentation of the applicant's health history transcript to the lawyer instead of presentation of a health history extract related to the dog attack was not excessive in this case and that there was no violation of the LLPPD.

The applicant appealed the decision of the SDPI before the Vilnius Regional Administrative County Court; however the Court rejected these arguments on the same basis as the SDPI. The applicant also appealed this decision, but the Supreme Administrative Court of the Republic of Lithuania (hereinafter – Supreme Administrative Court) rejected the applicant's appeal.

### Personal data collection by police for internal inspections

The SDPI received a complaint that the police illegally collected the complainant's personal data. The SPDI ascertained that the police received an anonymous report that a police officer (complainant's brother) in his request for reimbursement of travelling costs had indicated false data concerning his residence and vehicle data. According to this anonymous report the police started an internal inspection and checked the officer's personal data. It was determined that the vehicle for which the police officer had requested reimbursement was registered to the complainant and because of this the police checked the complainant's data in the Register of Motor Vehicles of the Republic of Lithuania in order to determine the motor vehicles that belong to the complainant.

The SDPI decided that such a collection of personal data of the complainant violated paragraph 1 of Article 3 of the LLPPD and issued an instruction. However, Vilnius Regional Administrative County Court rejected the SPDI arguments saying that the complainant's personal data were processed for the purposes of legitimate interests in order to carry out a detailed internal inspection. The SPDI appealed this decision and the Supreme Administrative Court upheld the appeal stating that the scope of the collected personal data did not meet the purpose of the internal inspection.

## C. Other important information

The SPDI is implementing the project 'Electronic service system of the SDPI'. The project aims to transpose four SPDI public services (two services for residents and two services for businesses) into the electronic environment and so improve the quality of the services, to develop data protection in the electronic environment and to contribute to the development of the information society.

# LUXEMBOURG

## A. Summary of activities and news

### Legislative changes

The law of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications was amended by a law dated 24 July 2010. This law implements the provisions of Directive 2006/24/EC on data retention into Luxemburgish law. It states that data are to be stored by the different national telecommunication service providers or network operators for six months. Upon judicial authorisation, they may only be accessed by law enforcement authorities for the needs of investigations, detection and prosecution of 'serious criminal offences', which are defined as offences entailing an imprisonment period of one year or more. The Grand-Ducal Regulation of 24 July 2010 contains a detailed list of the different data categories to be stored for mobile and fixed-line telephone communications as well as those pertaining to internet connections.

### Key topics

The *Commission nationale* advised the Luxembourgish Government on a vast array of legislative topics during 2010, among which the most important were the following:

- the aforementioned draft law implementing the provisions of Directive 2006/24/EC;
- the draft Grand-Ducal Regulation implementing a national pupil database held by the Ministry of Education;
- the draft law on electronic health records;
- the draft law implementing the provisions of Directive 2009/136/EC.

### News

The processing of sensitive data for medical and scientific research purposes took up a large part of the work of the Commission in the field of prior authorisation and guidance for data controllers.

The CNPD published general guidelines for the processing of citizen's data by local authorities. The DPA was also consulted in the context of the preparation of the general 'census' of the population to take place in early 2011.

On the matter of 'inadvertent' Wi-Fi data collection by Google, when driving for 'Street View', the national DPA decided to conduct an investigation, during which a Google Car was inspected with the help of an external specialist. The latter concluded that all the controversial equipment had been removed from the car. Furthermore, the national DPA received satisfactory answers to all the issues it had raised.

Throughout 2010, the national DPA had to intervene in multiple cases of data breaches or security shortfalls, including accidental transmissions of personal data to unintended recipients, data losses, data breaches relating to client files and many cases of website hacking (i.e. faulty security measures).

### Key events and awareness-raising

he CNPD continued its information and awareness-raising campaign throughout 2010. Besides a vast communication campaign launched for the European Data Protection Day, the *Commission nationale* participated actively in an awareness campaign on the security of passwords, together with the Ministry of Economy and Commerce. The CNPD also took part in the development of a brochure on 'How to protect your data on the Internet', specifically aimed at young children and teenagers. A total of 21 conferences and training courses were organised during 2010, as well as many meetings with public or private sector officials.

In order to increase the transparency towards the general public, the Commission asked all data controllers having obtained a prior authorisation for the purpose of video surveillance to use special labels designed by the CNPD. Such

information labels are to be placed next to the video surveillance panels, informing the public of the presence of such a surveillance system. The labels contain, among other things, the number of the authorisation, and they enable the public to verify in the public register the extent and limitations of the authorised data processing.

| Organisation | *Commission nationale pour la protection des données* (CNPD) |
|---|---|
| Chair and/or College | Mr Gérard Lommel – President<br>Mr Thierry Lallemang – Commissioner<br>Mr Pierre Weimerskirch – Commissioner |
| Budget | EUR 1 440 000 |
| Staff | College: 3<br>Legal department: 4<br>Notifications and prior checks: 2<br>General administration: 3<br>Communication and documentation: 1<br>Total: 13 |
| General Activity | |
| Decisions, opinions, recommendations | 436 |
| Notifications | 310 |
| Prior checks | 483 |
| Requests from data subjects | 242 |
| Complaints from data subjects | 145 |
| Advice requested by parliament or government | 6 |
| Meetings and consultations (public/private sector) | 110 |
| Information briefings and conferences | 21 |
| BCRs as lead DPA | 2 |

| | |
|---|---|
| Inspection Activities | |
| Inspections, investigations | 16 |
| Sanction Activities | |
| Sanctions | 3 |
| Penalties | N/A |
| DPOs | |
| Figures on DPOs | DPOs designated during 2010: 10<br>Total of DPOs designated (at date of report): 55 |

.

## B. Information on case-law

### Peace Court (*Tribunal de Paix*) in civil matters, on compensation for damage caused by an article published in a national newspaper

A communal employee's initials, profession, employer and job description were mentioned in a newspaper article which also linked the plaintiff directly to a drink driving offence. The court held that these citations constituted a breach of the plaintiff's privacy rights. Although this case does not directly invoke data protection law provisions, it may be regarded as constituting a precedent in the privacy field, as the judges established a test on how to reconcile a breach of privacy rights with the rights of the freedom of the press.

## MALTA

### A. Summary of activities and news

During the period under review no legislative amendments were introduced to the Data Protection Act and to the regulations made thereunder. This notwithstanding, this Office worked closely with the Malta Communications Authority with the objective of commencing the transposition exercise of Directive 2009/136/EC which amends, inter alia, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. A draft legal notice introducing the new and revised provisions was prepared, and was vetted by the Attorney General's Office, and was expected to be published in the second quarter of 2011. This joint transposition effort with the Malta Communications Authority was required, given that, in 2003, Directive 2002/58/EC was transposed, in part, under the Data Protection Act while the technical part was adopted under the provisions of the Electronic Communication Act.

There were two cases where an involved party felt aggrieved by the decision of the Commissioner and, in terms of Article 49 of the Act, made an appeal before the Data Protection Appeals Tribunal. In one case, the Tribunal decided in favour of the Commissioner. Given that the appellant did not appeal the Tribunal's decision within the stipulated timeframe, the case was considered as closed. In the other case, subsequent to the second sitting of the Tribunal, the appellant opted to withdraw the appeal and adhere to the directions issued by the Commissioner. The appellant honoured the Commissioner's decision and the case was closed.

Data controllers have also submitted requests for prior checking concerning the introduction of biometric systems at the workplace and the installation of CCTV camera systems and also in other areas where the processing operations involved particular risks of proper interference with the rights and freedoms of data subjects.

The Office has an obligation to promulgate data protection awareness for the benefit of the citizen and also for the benefit of the various sectors and data controllers. To achieve this objective, continuous work is undertaken to regularly hold presentations, give interviews to local newspapers and write newspaper articles. During this year, the Office delivered presentations to various entities on the applicability of the data protection rules in specific sectors. Among the presentations held were those for the Malta Employers' Association, the Malta Police, the Employment and Training Corporation, Young Enterprise and the University of Malta. During the year under review, the Office had the opportunity to contribute with a monthly article in the IT supplement of the Times of Malta. The articles tackled the data protection concerns applicable to various areas in the digital field, such as biometric devices, cloud computing, online behavioural advertising and CCTV cameras. Positive feedback has been registered from this awareness-raising initiative.

On 28 January, the Maltese Data Protection Authority joined the other Data Protection authorities to celebrate Data Protection Day. To mark this day on the local level, the Office of the Data Protection Commissioner distributed informative material to students in all state, private and church schools. This material had the main purpose of getting the message across and making citizens, particularly from a young age, aware of the inherent risks which one may be exposed to when providing personal information on the net. It has always been this Office's firm belief that for an effective culture change to happen there needs to be continuous investment in the young generation. It takes time to bring about such a change, but the consolidation of all the elements in the privacy formula will eventually yield the desired results. With the increasing available social networking applications, the privacy boundaries are being blurred and this Office is committed to strengthening the privacy objectives in this regard whilst being guided by the core concept of reasonable expectation to privacy.

During 2010, certain provisions of the Freedom of Information Act were brought into force. Under the same Act, regulations have also been published on applicable fees for access to documents, the timeframe during which a complaint or request for investigation may be lodged, and specimen application forms which will be used by the general public to submit requests for information. The remaining key provisions are expected to be introduced in the near future.

| Organisation | |
|---|---|

| | |
|---|---|
| Chair and/or College | Information and Data Protection Commissioner |
| Budget | EUR 290 000 |
| Staff | Professional Staff – 4<br>Technical Support – 2<br>Administrative Support – 2 |
| General Activity | |
| Decisions, opinions, recommendations | Decisions – 16 decisions / directions were issued in relation to formal complaints received by the Office.<br><br>22 opinions / recommendations were issued. These related to opinions issued in the form of newspaper articles which were intended for both the general public and data controllers, and other opinions or recommendations provided to data controllers on specific matters. |
| Notifications | 184 new notifications |
| Prior checks | 4 prior checking requests |
| Requests from data subjects | Queries received by phone – average of 35 calls on a weekly basis.<br>Queries received by email – 191. |
| Complaints from data subjects | 44 complaints |
| Advice requested by parliament or government | N/A |
| Other relevant general activity information | N/A |
| Inspection Activities | |
| Inspections, investigations | In total, 8 inspections were carried out in 2010:<br><br>3 inspections related to processing by law enforcement authorities and were centrally coordinated by the Joint Supervisory Authorities;<br>4 inspections were carried out in order to investigate specific complaints;<br>1 inspection was undertaken further to a request for prior checking. |

| Sanction Activities | |
|---|---|
| Sanctions | N/A |
| Penalties | N/A |
| DPOs | |
| Figures on DPOs | 22 Personal Data Representatives (PDR) were appointed in 2010. |

## B. Information on case-law

There was no new case-law during the period under review.

## NETHERLANDS

### A. Summary of activities and news

In order to be able to protect personal data in the most effective and meaningful manner, the Dutch DPA prioritises its work. This prioritisation is based on a risk assessment which our office carries out yearly and which is constantly updated following the signals we receive from various sources such as newspapers and the signal function for citizens on our website. In this risk assessment, the seriousness of the alleged offence, the number of individuals affected, the clarity of the indication of the breach and legal feasibility, and the effects of the large-scale use of new technologies are taken into account. The Dutch DPA in general focuses on strategic enforcement in order to achieve a higher level of overall compliance.

In 2010 the investigation the Dutch DPA undertook into hospitals' security measures regarding their patients' data was finalised. Following enforcement action concerning incremental penalty payments, the last hospital that had been inspected executed a satisfactory new risk analysis and in doing so complied with security norms for the health sector. After the hospital informed the DPA on the reparatory measures taken, the investigation could be closed. The Dutch DPA also investigated the collection and subsequent selling of sensitive data and profiles of persons who had visited a health related website.

The Dutch DPA also conducted investigations into, amongst other areas, the following data processing operations:

- the collection of Wi-Fi data by Street View cars of Google;
- the processing of personal data of students with a Public Transport Chip-card;
- the linking of data files by the social security investigation service;
- the input of police information in the Europol Information System;
- the use of Automatic Number Plate Recognition by two police forces;
- the exchange of patient data using regional electronic patient files.

Some situations required an immediate response by the DPA, as was the case when the Dutch DPA initiated discussions with the mayors of the towns of Ede and Enschede about the ethnic registration of Roma in their towns.

In addition to conducting investigations, the Dutch DPA advises the Government on draft legislation before bills are sent to Parliament. Following the advice from the Dutch DPA, proposals are (often) amended in order to avoid privacy violations. Amongst others, the legislative proposal for the introduction of smart meters was changed to the benefit of the consumer following the Dutch DPA's suggestions. The legislative proposal for the introduction of an alcohol-lock on cars was also amended to make sure data are not retained longer than necessary.

Lastly, the Dutch Cabinet that took office last year plans to present a renewed Dutch Personal Data Protection Act in line with the intentions of the previous Cabinet. The Dutch DPA has invested in an active contribution towards the consultation process preceding the draft legislation, in order to ensure a good bill will be drafted that is beneficial to the data subjects, the controllers and also the DPA itself.

| | |
|---|---|
| **Organisation** | Dutch Data Protection Authority |
| Chair and/or College | Jacob Kohnstamm, Chair.<br>Jannette Beuving, Member of the College and Vice-Chair.<br>Madeleine McLaggan, Member of the College. |
| Budget | Allocated: EUR 7 679 000<br>Executed: EUR 7 699 000 |
| Staff | 77 FTE (88 employees) |
| **General Activity** | |
| Decisions, opinions, recommendations | 775 (investigations, guidelines, code of conduct, prior checks, sanctions and advice in legislative process) |
| Notifications | 3 720 |
| Prior checks | 642 |
| Requests from data subjects | Issues signalled to the DPA through its website: 974.<br>Incoming emails: 2 814.<br>Incoming telephone calls: 2 417.<br>Of all these incoming requests, 172 complaints, 226 requests for information and 154 mediation cases were substantially dealt with. |
| Complaints from data subjects | Number of qualified complaints dealt with: 172 |
| Advice requested by parliament or government | 35 |
| Other relevant general activity information | |
| **Inspection Activities** | |
| Inspections, investigations | 60 |
| **Sanction Activities** | |
| Sanctions | 35 |
| Penalties | N/A |
| **DPOs** | |
| Figures on DPOs | 310 DPOs notified to the DPA |

## B. Information on case-law

### 1. Use of security cameras and their role in legal proceedings

An individual was seriously injured when a beer glass was slammed in his face in a bar. The incident was recorded by a security camera in the bar. When the police arrived on the same night, they watched the recorded material. The owner of the bar decided to keep the footage and store it on a disc supposedly to make sure the police would be able to view the footage again when necessary.

In this case the Court held that the owner of the bar was allowed to voluntarily provide the footage to the police on the basis of Article 8(f), in conjunction with Articles 9 and 43 of the Dutch Data Protection Act, in the interest of preventing, detecting and prosecuting crimes. The Court also held that a possible violation of the Dutch Data Protection Act, by making the footage available to the police contrary to the provisions of the Act, would not consequently make the use of the footage illegal in legal investigations, because the police would be able to request the footage by using Article 126nd of the Penal Code.

Furthermore, the Court held that in this case the data were not to be considered sensitive data in the sense of Article 126nf of the Penal Code, because the footage did not contain any more information than could have been seen by bystanders in the bar, nor did it contain additional information about the persons recorded.

This ruling by the Court is in line with the ruling of the European Court of Human Rights in the Perry vs. UK case, where the Court considered that normal use of security cameras in a public place did not lead to a violation of someone's private life.

### 2. The right to rectification

A person requested to receive the documentation that was used in drawing up an individual report, which was used in judging her application for a residence permit, and subsequently requested to rectify the documents and the individual report. This request was denied. The Council of State (highest Administrative Court) considered that the purpose of the right to rectification is not to correct or delete impressions, opinions, research results and conclusions in advice, with which the person concerned does not agree. In addition, the Council of State judged that by masking certain paragraphs in the individual report, the Minister of Justice could rightly invoke Article 43(e) of the Dutch Data Protection Act.

### 3. The right of access to, and rectification of, personal data

The Minister of Justice received a request from a natural person for access to and rectification of the data, both of himself and of a foundation, held by the Bureau BIBOB (BIBOB is the Law on the promotion of integrity for judgements by the public administration). The request with regard to the data concerning the foundation was denied, because a foundation is not a natural person and therefore Articles 35 and 36 could not be invoked. The access and rectification requests for the personal data of the person concerned were denied, because the Minister of Justice claimed that the BIBOB Law has a closed transfer regime and this would render the Dutch Data Protection Act inapplicable.

The Court however ruled that the BIBOB Law does not preclude requests made on the basis of Article 35 and 36 of the Dutch Data Protection Act, which the court inferred from the legal history. The Dutch Data Protection Act was therefore applicable. In addition, the closed transfer regime in the BIBOB Act is only applicable with regard to data of third parties and not with regard to the data held by the Bureau on the person requesting access and rectification him or herself. Therefore the Court ordered the Bureau BIBOB to reconsider the requests made by the applicant.

# POLAND

## A. Summary of activities and news

2010 was the 12th anniversary of the Act of August 29, 1997 on Personal Data Protection.

In 2010 a new Inspector General for Personal Data Protection (GIODO) was appointed. On June 25, 2010 the Sejm of the Republic of Poland appointed Dr Wojciech Rafał Wiewiórowski to this function. After approval by the Senate of the Republic of Poland, and after taking the oath on August 4, 2010, Dr Wojciech Rafał Wiewiórowski assumed the duties of GIODO, thus beginning his four-year term in office.

This was also the year of legislative work on the revision of the Polish Act on Personal Data Protection, which resulted in the enactment by the Sejm of the Act of October 29, 2010 amending the Act on Personal Data Protection.

The most significant changes introduced by the amending Act include new competences of GIODO including the power to impose fines as an enforcement measure in order to compel those entities that do not comply with the decisions of GIODO.

Also, an explicit right was added for GIODO to request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relative to personal data protection. Entities which received a formal position or request from GIODO are now obliged to respond to them within 30 days of their receipt.

The amended provisions of the Act on Personal Data Protection introduced a new type of crime, i.e. concerning preventing or hindering the performance of inspection activities of GIODO. The punishment for this crime is in the form of a fine, restriction of liberty or imprisonment of up to 2 years, and may be imposed not only on the data controller, but also on any person who, while participating in the inspection, prevents or hinders its conduct. The Act passed in 2010, amending the Law on Personal Data Protection, comes into force on March 7, 2011.

| | |
|---|---|
| **Organisation** | Bureau of the Inspector General for Personal Data Protection |
| Chair and/or College | Dr Wojciech Rafał Wiewiórowski, Inspector General for Personal Data Protection |
| Budget | PLN 13 842 000 |
| Staff | 127 |
| **General Activity** | |
| Decisions, opinions, recommendations | 1 412 administrative decisions issued, of which 879 concern personal data filing system registration, 137 concern inspections, 359 concern complaints, and 37 concern the transfer of personal data to third countries. |
| Notifications | 9 921 personal data filing systems registered. |
| Prior checks | As a result of registration procedures (prior checking), 1 650 personal data filing systems have been entered in the register of personal data filing systems; the processing of personal data filing systems containing sensitive data can start only after completion of the registration procedure. |
| Requests from data subjects | 3 448 legal questions |
| Complaints from data subjects | 1 114 complaints concerned infringements of personal data protection, including:<br>• public administration (149 complaints); |

| | |
|---|---|
| | • courts, the public prosecutor's office, the police, bailiffs (55 complaints);<br>• banks and other financial institutions (119 complaints);<br>• the internet (157 complaints);<br>• marketing (59 complaints);<br>• housing related (52 complaints);<br>• social, property, personal – insurance (28 complaints);<br>• Schengen Information System (38 complaints);<br>• telecommunications (57 complaints);<br>• employment (77 complaints);<br>• other (323 complaints). |
| Advice requested by parliament or government | 617 draft laws submitted for review to GIODO |
| Other relevant general activity information | 55 – number of training courses conducted by GIODO concerning provisions on personal data protection, especially for public institutions |
| **Inspection Activities** | |
| Inspections, investigations | 196 inspections, including:<br>• universities, higher education institutions (26 inspections);<br>• investment firms conducting brokerage activities (16 inspections);<br>• tax inspection offices (10 inspections);<br>• telecommunications service provider (14 inspections);<br>• municipal entities (16 inspections);<br>• insurance companies (12 inspections). |
| **Sanction Activities** | |
| Sanctions | In 2010 GIODO issued 23 notifications on suspicions of crime. No criminal sanctions have been imposed in relation to any entities by the courts. |
| Penalties | |
| **DPOs** | |
| Figures on DPOs | N/A |

.

## B. Information on case-law

An important decision was the order of May 12, 2010 (II SA/Wa 652/10) of the Regional Administrative Court in Warsaw, which upheld the decision of GIODO in the refusal to provide public information in the form of an inspection protocol of state enterprise utilities – declaring the application inadmissible and subject to rejection. GIODO had refused to disclose the public information on the basis of trade secrecy, which concerned the information requested.

The Supreme Administrative Court shared the position of GIODO that entities selling other people's products and services, in the case of a claim on these products or services, do not process personal data for marketing purposes on the basis of Article 23, paragraph 1, point 5 in conjunction with Article 23, paragraph 4, point 1 of the Act on Personal Data Protection (NSA judgment of January 5, 2010, case reference I OSK 399/09). The court found that a car dealer has the obligation to obtain consent for the processing of personal data for marketing purposes from potential customers, i.e. individuals who are interested in buying a car, but do not participate in the driving test. Data processing on the basis of a dealership agreement does not fall in the category of marketing of one's own products or services and therefore may not be based on Article 23, paragraph 1, point 5 of the Act (on Personal Data Protection), i.e. legitimate interest pursued by the data controller.

In another case, the Regional Administrative Court in Warsaw upheld the position of GIODO stating that from the moment a natural person is logged on to an account on a website, due to identification, the controller should take into account the objections raised by the data subject to the processing of personal data for marketing purposes, i.e. stop showing advertisements (Judgment of the Administrative Court in Warsaw on 15 June 2010, case reference II SA/WA 556/10).

## C. Other important information

In 2010 the Inspector General received **617 draft acts for an opinion**. The concerns of the data protection authority were raised by tendencies of different entities to form so-called mega-databases of personal data, containing information about millions of individuals. In 2010 GIODO issued opinions on legal acts, by virtue of which there are plans to introduce an information system in health care, called the Medical Information System (SIM), an Education Information System (SIO), which using a statistical collection of data is to become a filing system containing personal data, including sensitive data on preschoolers, schoolchildren, students and teachers, and a Central Register of Entities – National Register of Taxpayers involving partial 'duplication' and the wider availability of the Social Security database, in order to use it as a reference, also when dealing with tax authorities.

In 2010 GIODO took an active part in legislative work on legislation implementing the amended Act on the computerisation of entities performing public tasks, and work on the objectives of the Act on the provision of services by electronic means. This work drew particular attention to the compatibility of these draft regulations with general principles of data protection and the need to implement into Polish law the provisions of Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and related networks and electronic communications, Directive 2002/58/EC concerning the processing of personal data and privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for enforcement of consumer protection.

In 2010, GIODO examined the current state-of-play in relation to the protection of personal data processed in video surveillance systems, with the aim of initiating legislative action aimed at a comprehensive settlement of these issues. In so doing, GIODO will cooperate with the Ombudsman (RPO).

In 2010 more personal data filing systems were registered as compared to previous years (in 2008 – 3 760, in 2009 – 6 465, **in 2010 – 9 921**). This was possibly due to the fact that the declaration did not contain such a quantity of errors, as was the case in previous years. Undoubtedly, this result was influenced by the actions taken by GIODO that led to the modification of a computer program that assists filling the application form introduced on the basis of the Regulation of the Minister of Internal Affairs and Administration of December 11, 2008 as regards the template for notification of a data filing system for registration by the Inspector General for Personal Data Protection.

In 2010 GIODO continued educational activities, including:

- signing a memorandum of understanding (MoU) with the Internet Industry Employers' Association IAB Poland, which is aimed at ensuring that internet service providers in their activities adhere to privacy principles, in particular in the form of the joint development of a code of good practice. The mainstream media websites, as well as other companies in this industry, through this MoU, want to emphasize that they care about the proper protection of personal data, so that people using different content and services on the internet can feel safe;

- together with the Office of Electronic Communications (UKE), developing a 'Guide for users of publicly available telecommunications services', which aims at meeting the needs of people who intend to take a decision to make use of certain telecommunication services, as well as those who already use various forms of electronic communication;
- organising several conferences, including the conference entitled 'Reform of privacy', which officially initiated the public debate on how to protect privacy in the era of modern technology. This public debate is meant to develop a position on the changes to be made in Polish and EU legislation on data protection and privacy rights.

## PORTUGAL

### A. Summary of activities and news

This year was marked by the preparation of online notification procedures to be launched in January 2011. This involved developing the full electronic file, in order to significantly reduce the burden for data controllers of meeting obligations, as well as to shorten the reply period, without prejudice to proper assessment. The DPA's internal information system was also enhanced to allow a step forward towards the dematerialisation process, which was started a couple of years ago. It set up a management system to better handle the information requests from data subjects and data controllers, as well as the submission of complaints. All these technical developments were carried out by in-house experts, without the need to outsource these services.

The DPA decided to raise the notification fees from 2011, setting them at EUR 75 for a registration and EUR 150 for prior checking of data processing.

The increasing workload (almost 10 000 new proceedings) for the same staff level (28) and the extreme difficulty in increasing human resources due to restrictive administration rules should be pointed out.

On the other hand, a major amendment was introduced to the DPA's organic law, whereby the DPA's budget – until then coming entirely from the Parliament's budget – would have a split origin and would come partially from a Government department, as regards the amount corresponding to the DPA's own receipts. The DPA considered that this legal change has a very negative impact on the DPA's independence, as the uses of such funds are subject to an authorisation from a service directly reporting to the Government. Moreover, the amount still coming from the Parliament does not cover the DPA's expenses, which means that for the functioning of the DPA there is an unacceptable reliance on Government decisions. The DPA has full competences in the public sector, and should therefore not be limited in any way in the performance of its tasks.

The continuity of the Dadus project should also be highlighted – an awareness-raising project launched in 2008 for schools and targeting children 10-15 years old. It is based on a web platform where there is a variety of data protection content for youngsters, teachers and parents. The DPA developed a program to be used in classrooms, using multimedia supporting materials produced by the DPA and covering a set of themes.

In 2010, the DPA also launched a second contest for students on 'A Slogan for Privacy' and participated in dozens of school sessions. There are already more than 2 000 teachers registered in this project.

| | |
|---|---|
| **Organisation** | CNPD – *Comissão Nacional de Protecção de Dados* |
| Chair and/or College | Luís Lingnau da Silveira (Chair), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Durão Barroso, Luís Paiva de Andrade, Vasco Almeida |
| Budget | Budget allocated: around EUR 3.480 million (around EUR 2.140 million from the DPA's own receipt (fines and notification fees).<br>Budget executed: around EUR 2 million. |
| Staff | 28 |
| **General Activity** | |
| Decisions, opinions, recommendations | 7 120 decisions.<br>75 opinions issued on draft legislation by the Parliament or Government. |
| Notifications | 8 269 |

| | |
|---|---|
| Prior checks | 7 320 |
| Requests from data subjects | Around 5 600 by e-mail (this figure also includes requests from data controllers addressed to the Front Office).<br>Phone calls: around 11 000 (through the dedicated Privacy Line). |
| Complaints from data subjects | Around 200 (no exact figures available, as the complaints are included in the number of investigations started by the DPA).<br>Complaints mostly concern unsolicited electronic communications (e-mail and phone calls) and regard several kinds of employee monitoring at the workplace (video surveillance, abusive health tests, e-mail and internet control, installation of geolocation mechanisms in cars, such as GPS, and GSM mobile phones allocated to employees which they can take for personal use). |
| Advice requested by parliament or government | 83 requests for opinions.<br>Main issues dealt with: several bilateral agreements between Portugal and other states in the areas of: social security, tax and law enforcement cooperation; video surveillance in public areas; electronic surveillance within crime proceedings; databases of the Public Security Police; setting up of a central database of bank accounts within the fight against corruption; transposition of Directives 2006/123/EC, 2006/22/EC, 2008/48/EC and 2007/59/EC; relevant data protection matters in the State Budget; recording of phone calls in call centres; and general regulation of prison services. |
| Other relevant general activity information | Access and deletion requests for the Schengen Information System (SIS), a right used indirectly via the DPA: 149<br>Guidance activities for data controllers on specific data protection requirements covering the following matters:<br>• recording phone calls within three contexts (contractual relationship with clients, emergency calls and assessment of employees' quality performance in call centres);<br>• updating guidelines for health and security services at the workplace, following amendments to the Labour Code;<br>• alcohol and drug control tests at the workplace. |
| Inspection Activities | |
| Inspections, investigations | Investigations – 863<br>Inspections on the spot – 189 (both private and public sector) |
| Sanction Activities | |
| Sanctions | 248 fines |
| Penalties | EUR 507 291.69 imposed by the DPA |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

No significant case-law for the purpose of this report.

## C. Other important information

The DPA has been involved in many cooperation procedures as part of its own way of carrying out its mission.

Therefore, participation in national working groups should be underlined, such as the Secure Identity National Plan, the platform for health and security in the working environment, or the meetings held with several Government departments to discuss EU legal instruments being developed as well as regular contacts with other independent bodies working in similar areas to ours.

At international level, the DPA is a member of the Ibero-American Data Protection Network and co-organises with the Spanish DPA a yearly meeting to discuss issues of common interest.

The DPA also plays an active role in cooperation with other Member States in Schengen matters.

# ROMANIA

## A. Summary of activities and news

In 2010, the Supervisory Authority was confronted with both budgetary restrictions and the impossibility of filling all 50 staff positions provided by law. Another major problem is that (as at the time this contribution was provided) the supervisory authority is still confronted with a lack of suitable premises needed to ensure that the National Supervisory Authority for Personal Data Processing operates under lawful conditions.

During 2010 numerous legal persons of public and private law requested the point of view of the supervisory authority as regards the definition of data controller or data processor in view of the processing of personal data that they carry out, as well as with regards to the need to notify the processing of personal data carried out by data processors established on Romanian territory for data controllers established elsewhere within the European Union.

Information and points of view were also requested as regards the processing of biometric data (fingerprints) which were likely to be processed within a person's access control system. In the context of the legal provisions and of the need to ensure efficient protection of the right to intimate, family and private life with regard to the processing of personal data, the collection and processing of biometric data have been considered as excessive as compared to the stated purpose of processing and it was recommended to use alternative solutions in order to control employee access and register their working hours (for example by using a PIN code associated with other identification data of the employee).

As regards the transfer/transmission of data to other states, the majority of the cases resolved during 2010 related to the transmission of data to other EU Member States or to countries that ensure an adequate level of protection for personal data, also recognised by the European Commission.

The investigations carried out in 2010 by the Supervisory Authority related to infringements of the data subjects' rights, more exactly infringements of the right of access to data and of the right of opposition, as well as processing personal data within credit bureau type filling systems – the transmission of negative data to the Credit Bureau without prior information and other cases.

Based on the provisions of Article 21, paragraph 3, point h of Law No 677/2001 on the processing of personal data and the free movement of such data, the Supervisory Authority has issued a series of notices on draft legislative acts issued by various public institutions and authorities, as these referred to, amongst other aspects, issues on the collection and processing of personal data. During the course of 2010, the Supervisory Authority issued notices on 48 such draft laws, agreements, Government decisions, minister's orders, etc.

| | |
|---|---|
| **Organisation** | National Supervisory Authority for Personal Data Processing |
| Chair | Mrs Georgeta Basarabescu – President |
| Budget | Allocated budget: RON 3 679 000 – approximately EUR 876 000 |
| Staff | 46 positions occupied plus the two of the President and Vice-President |
| **General Activity** | |
| Decisions, opinions, recommendations | As in previous years, in 2010, both data subjects and data controllers requested the supervisory authority's opinion on the legal conditions on the processing of personal data.<br>A total of 250 such opinions were requested, which indicates an increased interest in respecting the legal provisions concerning the protection of personal data. |

| | |
|---|---|
| Notifications | 8 956 notifications were received from personal data controllers. |
| Prior checks | 1 preliminary control |
| Requests from data subjects | In 2010, the Supervisory Authority received:<br>50 requests for information (specific);<br>47 petitions.<br>These figures do not include phone enquiries. |
| Complaints from data subjects | 569 complaints |
| Advice requested by parliament or government | The Supervisory Authority has issued notices on 48 draft laws, agreements, Government decisions, ministers' orders, etc. |
| Other relevant general activity information | |
| Inspection Activities | |
| Inspections, investigations | 240 investigations |
| Sanction Activities | |
| Sanctions | 70 sanctions.<br>7 decisions to end personal data processing or delete the personal data which were processed. |
| Penalties | RON 59 600 – approximately EUR 14 200.<br>43 warnings. |
| DPOs | |
| Figures on DPOs | There are no legal provisions on such an institution within Romanian law. |

## SLOVAKIA

### A. Summary of activities and news

In 2010, the Office for Personal Data Protection of the Slovak Republic (hereafter referred to as 'the Office') continued its work on the formulation of new wording for the Data Protection Act currently in force. The draft law will amend the Data Protection Act taking into consideration recommendations resulting from the structured dialogue with European Commission representatives, incentives from the application of the Data Protection Act in practice as well as the latest developments following the launch of a comprehensive approach to the EU data protection framework. In December 2010, the draft amendment was submitted to the public, along with interdepartmental annotation procedures, and by the end of the year remained under the legislative procedures.

The Office was also confronted with a radical cut in its budget, some 23% less than the Office's budget in the previous year. The impossibility of fully covering employees' wages in the last quarter of the year even led to the request made by the Office to the Ministry of Finance to re-allocate the assets from the Office's capital expenditure saved from previous years towards payroll, which eventually took place, subject to agreed reservations.

The even lower budget was designed for 2011-13 under the pretext of the overall reduction in the expenditure of public administration bodies. The existing situation adversely affects the national supervision of the personal data protection and execution of the Office's tasks. Furthermore, due the continuous absence of the Office's representatives in the relevant working groups and conferences, it harms the Office's international reputation.

| | |
|---|---|
| **Organisation** | Office for Personal Data Protection of the Slovak Republic |
| Chair and/or College | Mr Gyula Veszelei |
| Budget | - EUR 728 696 |
| Staff | 34 |
| **General Activity** | |
| Decisions, opinions, recommendations | 467+16 based on the Public Access to Information Act |
| Notifications | 40; as well as notification of PDPOs (personal data protection officials) – 1020 |
| Prior checks | 0 |
| Requests from data subjects | 483 |
| Complaints from data subjects<br>Complaints from other subjects | 121<br>35 |
| Advice requested by parliament or government | 85 |
| Other relevant general activity information | Inspection proceedings – 277<br>Examination of notifications – 324<br>Office´s orders binding for individual controllers – 144 |

| | |
|---|---|
| | Decisions upon lodging of objections against Office´s decisions – 12<br>Cross-border data flows – 11 decisions upon approval of international transfers to third countries<br>Criminal filing – 3 |
| Inspection Activities | |
| Inspections, investigations | 125; 73 submissions for explanations;<br>Extra:<br>*Ex officio* inspections – 121<br>Key topics and issues:<br>• leakage of personal data from health care providers, especially from maternity hospitals for the purposes of newborn insurance;<br>• infringements caused by satellite and cable TV providers and providers of cartographic and geodetic services;<br>• insufficiency in the provision of information to data subjects in online commerce;<br>• incorrect information provision side of loyalty card issuers;<br>• illicit copying and scanning of personal documents;<br>• inappropriate marking of the area put under video surveillance;<br>• collection of personal data excessively beyond the original purpose of processing and for incompatible purpose. |
| Sanction Activities | |
| Sanctions | 21 |
| Penalties | EUR 60 578 |
| DPOs | N/A |

## B. Information on case-law

In 2010, three applications were made to the court for judicial review of decisions issued by the Office. One controller of an information system processing data for the purposes of online commerce sued the Office because he was sanctioned by the office for not providing the necessary cooperation to the Office. The fine imposed on him was of a disciplinary nature. The Office's decision is currently being reviewed by the court of first instance.

The subject matter of the other two cases was 'measures for remedy' imposed upon a controller, and their lawfulness. In one case, the Office obliged the controller (Bratislava county – Old town) to destroy the personal data of the data subjects published on its web page without legal grounds. The court of first instance has not ruled on the matter yet. In another case, the Office required that the controller (the multimedia publishing store) destroy a data subject's personal data of a sensitive nature (health data) which had been published in a weekly society magazine. In this particular case, the court did not issue a final verdict either.

# SLOVENIA

## A. Summary of activities and news

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). In 2010 the Commissioner initiated 599 cases regarding a suspected breach of the PDPA provisions, 202 in the public sector and 397 in the private sector. In the public sector the most common suspected breaches involved unauthorised transfer of data to third persons, unlawful publication of data, unlawful collection of data, denied access to a data subject's data and inappropriate security of data. In the private sector most suspected breaches involved abuse of data for the purpose of direct marketing, unlawful collection of data, unlawful publication of data, unlawful video surveillance and transfer of data to unauthorised third persons. The Commissioner issued sanctions for 179 offences. The number of inspection and offence procedures was similar to the previous year.

In addition to the inspection and offence authority competencies, the Commissioner performs other tasks as provided by the PDPA. The Commissioner issues non-binding opinions and clarifications on specific issues regarding data protection raised by individuals, data controllers, public bodies and international bodies. In 2010 the Commissioner issued 1 859 opinions and clarifications, which shows a significant increase from the previous year (1 334) and may be attributed to the transparent work and intensive public campaigning of the Commissioner. The Commissioner is, under the PDPA, also authorised to conduct prior checks regarding biometric measures, transfer of data to third countries and connection of filing systems. The data controllers in such cases need to firstly obtain the Commissioner's permission. The number of prior checks has not increased from the previous year.

In the course of its awareness-raising activities the Commissioner continued its preventive work (lectures, conferences, workshops for different public groups). Together with the Centre for Safer Internet of Slovenia, the Commissioner covered awareness-raising activities for children and young people (lectures at schools, publications). The Commissioner published four guidelines on different data protection topics covering online forums, privacy impact assessments, guidelines for healthcare service providers, and guidelines for information solution developers, and published two brochures on patient data and on data protection for consumers. In the context of European Data Protection Day, the Commissioner organised a round table debate that focused on direct and targeted marketing done by retailers that often invade the rights of consumers. On this occasion the Commissioner conferred awards on three data controllers for good practice in personal data protection – one of the awards being dedicated to efforts for respecting the Privacy by Design principle. 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 Commissioner participated in a number of inter-departmental work groups on e-government projects, such as e-Health, e-Social services, e-VEM (portal for entrepreneurs) and e-archiving, and in the inter-departmental work group for the strategy for developing the information society 2011-15. The Commissioner was consulted by the legislator and competent authorities regarding 51 Acts and other legal texts. The Commissioner also participated in a number of international bodies: 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, and 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 continued her work as the Vice-President of the Joint Supervisory Body of Europol.

| | |
|---|---|
| **Organisation** | Information Commissioner of the Republic of Slovenia |
| Chair and/or College | Mrs Nataša Pirc Musar |
| Budget | EUR 1 500 000 |
| Staff | 33 employees: the cabinet (4), administrative (3), access to public information legal advisors (11), data protection researchers and advisors (5), data protection supervisors (10) |
| **General Activity** | Data protection and access to public information |
| Decisions, opinions, recommendations | 575 opinions and recommendations based on requests from data subjects or data controllers |
| Notifications | 250 notifications on personal data filing systems |
| Prior checks | 25 prior checks: 8 on biometrics, 10 on transfer of data to third countries, 7 on connection of filing systems |
| Requests from data subjects | 1 859 requests for opinions/clarifications from data subjects |
| Complaints from data subjects | 628 complaints from data subjects altogether.<br>477 complaints qualified: 102 unlawful collection of data, 101 unlawful transfer of data, 90 unlawful publication of data, 86 direct marketing, 85 denied access of data subject to data, 59 video surveillance, 47 data security, 58 other. |
| Advice requested by parliament or government | The legislator and competent authorities drafting the legislation consulted the Commissioner regarding 51 acts and other legal texts, including the Privacy Protection Act, Criminal Procedure Act, Foreigners Act, State Prosecutors Act, Drivers Act, Insurance Act, Banks Act, Act on Gambling, Act on Protection in Road Traffic, etc. |
| Other relevant general activity information | The Commissioner in 2010:<br>• continued its preventive work (lectures, conferences) together with the Centre for Safer Internet of Slovenia;<br>• participated in a number of inter-departmental work groups on e-government projects, e-social services, e-health, e-archiving, etc.;<br>• published 4 guidelines on different data protection topics: online forums, privacy impact assessments, guidelines for healthcare service providers, guidelines for information solution developers; published 2 brochures: patient data and data protection for consumers. |
| **Inspection Activities** | |
| Inspections, investigations | 599 inspections: 202 in the public sector, 397 in the private sector. |
| **Sanction Activities** | |

| | |
|---|---|
| Sanctions | 179 offence procedures initiated (45 in the public sector, 82 in the private sector), of these 36 warnings, 81 admonitions, 35 fines and 10 payment orders were issued. |
| Penalties | The DPA imposed EUR 157 417 in penalties. |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

The Ljubljana public transportation company (LPP) introduced an ***e-ticketing system, based on the use of an anonymous or a personalised electronic travel card***. The company also processes passengers' location data (data on the time and place of entering the bus and data on the bus line the passenger took). The Commissioner established that in the case of a personalised travel card it is not necessary for the company to process location data as the passenger is charged a fixed monthly fee. The company did not obtain consent from the passengers and the Commissioner thus concluded that the company processed the above location data without an appropriate legal basis. The company was ordered to delete the collected location data and to adapt the system in order to no longer process such data in the future.

The Commissioner received a complaint from an individual who joined an SMS club, then soon deregistered but still received commercial content. The company operating the SMS club argued that a mere ***mobile telephone number cannot be treated as personal data*** as it points to a device and not necessarily to a person. The Commissioner established that a mobile phone number must be regarded as personal data, as the individual is identifiable, taking into account all the means the data controller can reasonably use in order to identify the individual. Direct marketing via SMSs is only permissible with the individual's consent and the data controller must delete or render anonymous the data on individuals who have cancelled their registration. The Administrative Court later upheld this decision.

A newspaper distribution company introduced ***GPS monitoring of individuals who distribute newspapers***. The company obtained the employees' consent, however if the employees did not carry the device the company would terminate their employment. The Commissioner established that GPS monitoring in this case constitutes data processing, and that the company did not demonstrate an appropriate legal basis for such processing. Processing personal data on the basis of personal consent is not sufficient in employment relationships, where the employer is the stronger party and the employee cannot give valid consent if threatened with the termination of the employment contract. The Commissioner ordered the company to stop using the GPS devices for this purpose.

A municipality started ***reviewing video surveillance footage to detect violations in stationary traffic (illegal parking)***. The city traffic wardens did not determine violations 'on the spot' but rather reviewed video surveillance footage and checked for possibly illegally parked or stopped vehicles. The traffic wardens would then establish the identity of the driver and send him or her a ticket. The Commissioner found that such conduct is disproportionate and, more importantly, without legal grounds. The Information Commissioner prohibited the municipality from reviewing footage of the video surveillance system for the purpose of offence proceedings.

The Commissioner received a considerable number of complaints regarding the ***publication of personal data in the media, on the internet, and especially on social networking sites***. The Commissioner is only competent to act in cases that concern data that are part of a filing system. That is why in most cases (e.g. the existence of defamatory content on online forums, false profiles on social networks) the Commissioner only advises the individuals to complain to the police or state prosecutors competent to take action. The act of misusing personal data is a criminal offence as determined by the Penal Code of Slovenia. The injured party may also initiate a civil action before a court. In cases where such publication involves data from filing systems (such as the publication of criminal charges, medical records, etc.) the Commissioner initiates an inspection procedure.

## C. Other important information

The Commissioner was also active in the field of bilateral international cooperation. In 2010 the Commissioner hosted a study visit by Polish, Hungarian and Kosovar representatives, and an official of the European Fund for the Balkans.

In a consortium with the Ludwig Boltzmann Institute for Human Rights from Austria, the Commissioner participated in a twinning project – Implementation of a Personal Data Protection Strategy in Montenegro. The project focused on establishing a national supervisory body for data protection and also establishing and implementing the legal framework for data protection in Montenegro.

In terms of policy issues the Commissioner has dealt with extensively, it is necessary to mention the increasing use of video surveillance, in response to which the Commissioner has proposed changes to the existing legislation which would better protect individuals' rights in this regard. The Commissioner also notes that smart face recognition video surveillance is developing fast. Regarding the IT solutions in private companies and the public sector the Commissioner notes that security of such systems is often not comprehensive enough to satisfy the conditions set by the PDPA. An important issue, raising many concerns, is also the employees' right to privacy and data protection in the workplace, in response to which the Commissioner proposed a draft of an Act on Communication Privacy in the Workplace. Special attention was paid by the Commissioner to endorse and educate data controllers on the concept of Privacy by Design, namely in the projects of switchover to electronic commerce, the Security Information and Event Management tools, and the introduction of average speed cameras on the roads. The Commissioner also pays special attention to the development of Cloud Computing, which raises significant concerns in terms of data security and responsibilities of the data controller, and the so-called Internet of Things.

# SPAIN

## A. Summary of activities and news

In order to make it easier for controllers and processors to comply with the Organic Law on the Protection of Personal Data and its implementing regulation, a self-assessment tool, EVALÚA, was added to the agency's website; this allows the user to check compliance with the law, assess the security measures laid down in the regulation, and obtain a report detailing any deficiencies detected, so that, if necessary, the relevant corrective measures can be taken. By the end of 2010, EVALÚA had been accessed 20 294 times.

The agency has continued with its policy of informing experts and individuals bound by the LOPD by holding the 3rd Open Annual Session of the AEPD, which was attended by over 800 people, and it has expanded the catalogue of informative guides about the LOPD with the publication of the 'Guide to RFID Technology Security and Privacy', in collaboration with the National Communications Technology Institute (INTECO), and by re-editing the 'Guide to Security'. This includes a model 'Security Document', which serves as a guide and facilitates implementation of the rules on data protection and compliance with them.

Furthermore, the General Judicial Council and the AEPD signed a collaboration agreement which establishes a protocol for carrying out inspections regarding data protection in judicial bodies, as well as implementing initiatives which promote effective application of the rules on data protection in the legal authorities as a whole.

Along the same line, in view of the importance of health data, the AEPD adopted the initiative of drawing up a 'Report on compliance with the LOPD in hospitals', given the discovery of a growing amount of cases of infringements of the LOPD, principally linked to breaches of the duties of security and secrecy provided for under the LOPD. The assessment was carried out by sending a questionnaire to more than 600 centres included in the national register of hospitals, which was answered by 92% of them, and by following up on the responses given by the addressees.

Furthermore, the AEPD has continued to have contact with key social networking sites such as Tuenti and Facebook, to improve their privacy policies and prevent minors under the age of 14 from gaining access to such networks.

In June 2009 the AEPD was awarded the lead in a Twinning project to be developed in Croatia. This project aims to work with the Croatian Agency for Personal Data Protection to prepare its entry into the EU. The EU provided EUR 1 350 000 of funding for this and it is expected to last 22 months. In 2010, the Twinning project with the State of Israel was successfully concluded; AEPD was elected to lead this project which lasted 20 months.

As can be seen in the table below, there has been an intensification of registration and inspection activities.

| | |
|---|---|
| Organisation | Spanish Data Protection Agency |
| Chair and/or College | Mr Artemi Rallo / Mr José Luis Rodriguez (since June 2011) |
| Budget | EUR 15 425 160 |
| Staff | 147 civil servants + 7 non civil servants and 1 Commissioner |
| General Activity | |
| Decisions, opinions, recommendations | Number of decisions regarding claims: 6 189; Reports: 120 |
| Notifications | 623 148 registration operations (public and private files).<br>Total of notified files: 2 144 872 (+ 31%). |
| Prior checks | N/A |
| Requests from data subjects | 104 826 requests via the Help line (in writing, by phone, by the web and the front desk) (+ 8.2%).<br>597 report requests sent to the Legal Department (298 from public administrations and 229 from citizens or companies). |
| Complaints from data subjects | 4 300 complaints from data subjects. Sectors such as telecommunications and video surveillance sectors (29% and 14% respectively), internet and advertising, etc. |
| Advice requested by parliament or government | The AEPD issued legal opinions on a total of 97 general provisions, including the Sustainable Economy Bill, the Civil Registry Act, the Consumer Credit and Gambling Regulation Act, as well as draft Royal Decrees. |
| Other relevant general activity information | 2 499 179 acts of accessing via the web (7 619 daily average).<br>2 508 850 consultations of the public register.<br>560 authorisations of the Director for International Transfers. |
| Inspection Activities | |
| Inspections, investigations | 4 302 previous investigations and 1 643 claims of the data subject.<br>6 189 Resolutions from inspection procedures divided into (+ 5.76%): – 1 830 Protection of rights claims (access, rectification, erasure and objection) – 4 359 Procedures relating to the sanctioning power.<br>The inspections department has acted not only in response to specific problems but also *ex officio* in different areas:<br>• data protection in hospitals;<br>• transfer of business data;<br>• inspections on the sale of debt by telecommunications operators and financial institutions;<br>• inspection of the Schengen system in Spain; |

| | |
|---|---|
| | • analysis of contractual clauses of telecommunication operators;<br>• investigation of the access criteria based on legitimate interest in the Register of real estate, Register of vehicles and Cadastral register. |
| Sanction Activities | |
| Sanctions | 591 sanctioning resolutions; 92.49% relating to the Data Protection Act; 7.23% the Act on Internet Society Services (spam); 0.28% the Act on Telecommunications (advertising, fax) |
| Penalties | EUR 17 497 410.02 (-29.65% with regard to 2009) |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

The 'right to be forgotten' on the internet has become one of the most hotly discussed topics in the area of new internet services. The Spanish Data Protection Agency has responded to the public's complaints relating to services rendered by multinationals by taking the view that the Spanish Data Protection Act is applicable in cases where a combination of elements such as the use of means in Spain, the existence of an establishment and the targeting of users occurs. Appeals against some of the rulings have been brought before the *Audiencia Nacional* (Spanish central court), though no decisions have yet been announced.

The Spanish DPA was one of the signatories of a joint letter from various authorities of different regions to Google Inc. regarding Google Buzz. With this and other examples, the Agency, working together with other authorities, has thus made a commitment to taking a step forward in the protection of internet users. This step forward has also led to the investigation of alleged legal breaches. In October 2010, the AEPD began a sanctioning procedure against Google Inc. and Google Spain for collecting and storing information on Wi-Fi networks via the vehicles used for the Street View service. Inspections on Facebook also began in October and involved requesting information about whether users in Spain had been affected by the disclosure of data to advertisers or other companies by any of the most popular applications on Facebook. In November similar actions were begun regarding MySpace.

### Resolutions of the AEPD:

→ The right of erasure of personal information in a blog of Google's Blogger platform was confirmed. The AEPD considers in this case that the personal information must be deleted as the freedom of expression has limits on other rights. Regarding this point, the National Court considered that if the information disclosed has no public relevance, data protection rights will prevail. While the search engine is not responsible for the contents of the blogs of its platforms, it has to order their withdrawal or make access impossible when the AEPD, as the competent authority, determines so and when they have effective knowledge (TD/00242/2010 and TD/00021/2010).

→ Sending commercial mass emails without using BCC and disclosing the addresses. This entails two infractions. On the one hand it is considered unsolicited email (spam) and a breach of Article 21 of the LSSI. On the other hand, the e-mail address is considered personal data and sending an email disclosing several addresses to different recipients without their consent is considered a breach of Article 10 of the LOPD covering violation of the secrecy and confidentiality of data (PS/00228/2010).

### Case-law: National Court

- The ruling of the National Court of February 10, 2010, considers that the duty of secrecy was breached by an official newspaper in publishing a decision from disciplinary proceedings against a civil servant, including details of the charges, the specific information on the basis of which the penalty was imposed through a criminal case brought against that official, as well as a literal disclosure of the complainant's criminal conviction, thus revealing the crime and sentence. It was understood by the National Court that these data were excessive for the intended purpose of the publication.
- The ruling of the National Court of February 23, 2010 considers the prevailing right to freedom of information in cases of publication in digital newspapers of data relating to the salaries and contracts of the manager of a public company and his spouse.

### Case-law: Supreme Court

- The ruling of the Supreme Court of June 2, 2010 confirms the doctrine currently existing in relation to breach of secrecy in the case of documents appearing in streets, in that the infringement is attributable to the appellant company if the documentation was abandoned by a third party who subsequently showed that he had been working for that company.
- The rulings of the Supreme Court of July 22 and October 5, 2010 emphasize the need for a contract for services of a processor to be included in a contract and put in writing or by other means to prove its contents, according to Article 12.2 of the Data Protection Act, which was not the situation in the case under consideration.

Three judgments of July 15, 2010 are particularly relevant to resolving the appeals filed against the regulations implementing the Data Protection Act as well as two preliminary judicial rulings, related to Article 10.2 b) of the aforesaid regulation (referring to legitimate interest). The Supreme Court fully endorses the regulation, annulling only 5 of the 158 items that comprise it, not judging Article 10.2.b and increasing legal certainty in the Spanish system of data protection[7].

[7] More information can be found at the following link (in Spanish)
https://www.agpd.es/portalwebAGPD/jornadas/3_sesion_abierta_2010/common/SESION_ABIERTA_2010_SEGUNDA_PARTE.pdf

# SWEDEN

## A. Summary of activities and news

### Legislative developments

#### *Amendments to the Swedish Constitution*

During 2010 quite a few laws were introduced and bills submitted that all had an impact on privacy. Among other things the Riksdag (the Swedish Parliament) on 24 November voted for a number of amendments to the Constitution including one strengthening the protection of privacy. This amendment is meant to ensure that the State and municipalities do not introduce new comprehensive databases without explicit legal grounds and an assessment of whether or not the legislative measure is proportionate having regard to the infringement of privacy. This amendment is a result of the criticism expressed by a Government Committee – Committee on the protection of privacy – after an extensive survey and analysis presented in two reports from 2007 and 2008. The Data Inspection Board has over the years seen many examples of legal drafting where privacy analyses are completely missing or are very poor.

#### *The Credit Information Act*

In earlier reports we provided information on the *Credit Information Act* and the fact that an amendment to the *Fundamental Law on Expression* (a constitutional law) in 2003 had led to the possibility to disclose credit information on websites to anyone without having to comply with the strict rules of the *Credit Information Act.* This led to infringements of privacy and many complaints. In June 2010 the Riksdag approved the Government's proposal for changes to the *Credit Information Act* aiming at providing better protection for individual persons on the internet.

#### *The Data Retention Directive*

The *EC Directive on the retention of data processed in connection with the provision of public electronic communication* has still not been transposed into Swedish law. The Swedish Government has presented a bill on the retention of traffic data for law enforcement purposes in order to implement the Directive in Sweden. However, a minority consisting of three parliamentary parties pushed through a minority planking under Chapter 2, Section 22 of the Instrument of Government (one of the fundamental laws). This meant that the bill could not be approved by the Riksdag until March 2012.

### Supervision activities and other issues of interest

#### *The Signals Intelligence Act*

On 12 February 2009 the Government commissioned the Data Inspection Board to examine how the National Defence Radio Establishment (FRA) handles personal data in connection with signals surveillance for defence intelligence activities. The background is that a new *Signals Intelligence Act* came into effect on 1 January and although there are a number of rules in the law designed to protect privacy, the Riksdag required further control mechanisms. The Data Inspection Board reported its findings to the Government in December 2010. Our office analysed, inter alia, what privacy problems may arise in connection with the signal intelligence activities of the FRA. The Data Inspection Board also investigated the procedures and guidelines used in these activities to see if they are sufficient to handle such problems. The FRA has, after remarks from the Data Inspection Board, made improvements to its procedures for how personal data should be handled. The FRA has, among other things, introduced systematic and recurring log audits that enable follow-up on incorrect or unauthorised access to personal data.

#### *Supervision of the current system for national electronic identification (e-id)*

The Swedish National Audit Office has stated that the supervision of the current system for national electronic identification (e-id) is insufficient. Information security audits have not been performed across the entire chain of events or on all parties involved in issuing or verifying an e-id. The Data Inspection Board has initiated a project

that aims at understanding the different steps involved in issuing an e-id and at mapping the stakeholders involved, for instance data controllers or data processors. The project includes a number of inspections of issuers (for instance banks) and users (for instance public authorities) to see if the e-id system is compliant with data protection rules.

*Website against violations on the internet*

At the beginning of 2010, the Data Inspection Board launched a website – kränkt.se or krankt.se – aimed at young people, giving them advice on what to do if there has been a violation on the internet.

*Privacy Year Report*

Again, the Data Inspection Board produced a privacy report ***Privacy Year 2010*** which, like the two previous reports, contains a comprehensive survey of new legislation, proposals, decisions and techniques that affected privacy during the year.

| | |
|---|---|
| Organisation | Data Inspection Board |
| Chair and/or College | The Data Inspection Board is led by the Director General. There is also an Advisory Committee consisting of five members. |
| Budget | EUR 3.3 million |
| Staff | 44 (27 with legal degrees, 4 IT specialists and 1 HR, 2 communications and 10 administrative staff) |
| General Activity | |
| Decisions, opinions, recommendations | Guidelines on whistleblowing; Checklist on the use of positioning techniques; Report on how to handle and protect sensitive personal data within private insurance companies; Recommendations to the Government with regard to IMI. |
| Notifications | 289 – it should be added that the Swedish legislator has made use of almost all possibilities to make exemptions from the notification requirement. |
| Prior checks | 344 |
| Requests from data subjects | 2 100 e-mail and 5 300 telephone questions respectively regarding the Personal Data Act; 527 telephone questions regarding the Credit Information Act; 884 telephone questions regarding the Debt Recovery Act. |
| Complaints from data subjects | 332 relating to the Personal Data Act; 18 relating to the Credit Information Act; 154 relating to the Debt Recovery Act. |
| Advice requested by parliament or government | 74 consultations and 50 informal consultations with regard to bills with possible impact on privacy. |
| Other relevant general activity information | The Data Inspection Board has issued a new administrative rule with regard to whistleblowing and dealt with more than 70 consultations with data protection officers and about 10 BCR as part of the cooperation |

| | |
|---|---|
| | procedure (not lead). |
| Inspection Activities | |
| Inspections, investigations | 210 inspections – examples of key topics: money laundering, social media, positioning technology in working life, camera surveillance, eCall, police databases and the pharmacy market. |
| Sanction Activities | |
| Sanctions | None in 2010 |
| Penalties | N/A |
| DPOs | |
| Figures on DPOs | Total number of notifications of DPOs: 6 442, of which 206 were new ones in 2010. The total number of DPOs amounts to 3 828 (one DPO may have several DPO commissions). |

## B. Information on case-law

### The Swedish Supreme Administrative Court's decision regarding the publication about bankruptcy creditors on the internet

This case involved the application of Section 10 f) of the Personal Data Act concerning weighing the interest of the controller and the data subject respectively. A consultancy company had – on its website – published the names, addresses and deposit amounts of a great number of creditors as well as information about the debtors of a finance company which had gone bankrupt. The data subjects had not given their consent to the publication, and the Supreme Administrative Court stated that the publication on the internet made the information very easy to access and disseminate extensively. The Court ruled that the interest of the controller of personal data was not of greater weight than the interest of the data subjects in protecting their privacy.

### Decision of the Administrative Court of Appeal regarding electronic keys

A housing firm had introduced a system with electronic keys to be used by residents to unlock doors to and within buildings. The electronic key is linked to a certain flat and leaves data in a passage log showing when and where the resident uses the key. One of the purposes for which the logs were used was to control who had accessed the laundry room, in order to deal with problems that had arisen there. For this processing of passage logs, there was no consent. The Court found, as did the Data Inspection Board, that the interest of the data subjects in protection of their privacy had greater weight than the interest of the controller, the housing firm, to cope with the problems in the laundry room.

### Decision of the Administrative Court of Appeal regarding the use of SMS provided by the Social Insurance Office

The Data Inspection Board had ordered the Social Insurance Office (the Office) to carry out an analysis of the risk and vulnerability of, inter alia, the use of SMS provided by the Office for notification about temporary parent allowances. The Office argued that it had no obligation to carry out the analysis, since it was not the controller of data before the information via SMS had reached the place of reception on their website. Both the Data Inspection Board and the courts of law found that the Social Insurance Office was to be considered as the controller of data already when the individual persons sent the information. The Administrative Court of Appeal stated that the Data Inspection Board, in its capacity as supervisory authority, in individual cases must decide on the security measures

that the controller of data has to take. The Court found that the analysis in question was such a measure, and that the analysis would not be costly or in any other way inappropriate.

### Decision of the Administrative Court regarding whistleblowing

A company had applied for permission from the Data Inspection Board to process personal data in a whistleblowing system. The application was granted but only to a certain extent and on certain conditions. One of these conditions was that processing of personal data concerning legal offences may only refer to persons in key positions or a leading position within the company. The company appealed against this limitation and claimed that all employees should be included in the reporting system. The Court first stated that the processing concerned extremely sensitive personal data; it deals with reports about suspected legal offences. The Court found after a balancing of interests that the company's interest was not of greater weight than the interest of the data subjects as regards protection from infringements of privacy.

### Decision of the Administrative Court regarding video surveillance of employees

A public transport company had, for one month, carried out video surveillance in one of its bus depots in order to cope with serious problems such as, for instance, sabotage of the buses and ticket machines. The place of work in question had about 600 employees and at most 1% of them were involved in the criminal activities. The Court found that the video surveillance had especially infringed privacy since there was no information of any kind on the surveillance. It further stated that the surveillance had resulted in an encroachment on the data subjects' privacy that was not proportionate to the purposes of the surveillance.

## C. Other important information

During 2010 the number of inspections increased considerably.

In 2010 the Riksdag decided to increase the budget of the Data Inspection Board by almost 10%.

# UNITED KINGDOM

## A. Summary of activities and news

January: The Coroners' and Justice Bill receives royal assent, providing the ICO with the power to audit central Government departments without consent.

We mark European Data Protection Day by launching the Think Privacy campaign and promoting the 'i in online' project.

February: In preparation for our report to Parliament on the state of surveillance we appoint the Surveillance Studies Network to report on development in surveillance in the UK since 2006.

We serve an enforcement notice on the Labour Party after it breached the Privacy and Electronic Communications Regulations by making unsolicited automated marketing calls.

March: We host the Data Protection Officer conference in Manchester.

We publish The Privacy Dividend report, which provides organisations with a financial case for adopting data protection best practice.

April: Our new powers come into effect, enabling the ICO to impose monetary penalties for serious breaches of the Data Protection Act.

We issue data protection guidance to political parties and candidates in the run up to the general election.

July: We launch our new Personal Information Online code of practice, providing good practice advice for organisations doing business online.

We launch a campaign to remind private medical practitioners to notify the ICO about where they are processing personal information. Over 3 300 new notifications are received as a direct result of our campaign.

August: We remind letting and estate agents that they risk legal action if they fail to notify the ICO. Nearly 1 000 new notifications were received as a direct result of our campaign.

We commission a Review of Availability of Advice on Security for Small and Medium-sized Organisations, to better understand how they access advice for protecting personal information.

September: We host a delegation from Macedonia, whose members were seeking advice on implementing and regulating data protection regulation.

We host the European Case-handling Workshop in Manchester, with 50 representatives from 29 countries and territories across Europe.

October: Local MP and Chancellor of the Exchequer George Osborne officially opens the extension to our head office, bringing all the ICO's Wilmslow staff under one roof.

We serve our first two monetary penalties against private company A4e and Hertfordshire County Council for serious breaches of the Data Protection Act.

Google Inc. signs a commitment to improve data handling to ensure breaches like the collection of Wi-Fi payload data by Google Street View vehicles do not occur again.

November: We provide an update to Parliament on the state of surveillance, noting that new laws that impact on privacy should undergo post-legislative scrutiny.

We successfully prosecute two former T-Mobile employees for offences under Section 55 of the Data Protection Act, under which it is an offence to obtain, disclose or sell personal data without the data controller's consent.

December: We remind schools not to hide behind data protection myths to prevent parents from taking photos at school nativity plays, generating over 100 pieces of media coverage.

We issue a response to the Government's announcement on the Protection of Freedoms Bill.

More details of our activities during 2010 can be found in our annual reports for 2009/10 and 2010/11, which are published on our website www.ico.gov.uk.

Figures are for the UK financial year April 2010-April 2011 unless otherwise stated

| | |
|---|---|
| Organisation | Information Commissioner's Office |
| Chair and/or College | Christopher Graham, Information Commissioner |
| Budget | GBP 20 172 000 approximately |
| Staff | 351 (327 full-time equivalent; also includes FOI and other non-DP staff, e.g. Facilities, Finance, HR) |
| General Activity | |
| Decisions, opinions, recommendations | 36 public statements on things other than guidance and enforcement action. Included statements on Google, privacy/DP rights/obligations awareness, changes to ICO and DP law (e.g. cookies).<br>3 codes of practice (personal info online, data-sharing, assessment notices).<br>55 sanctioning proceedings (see below) and associated media statements. |
| Notifications | 339 298 |
| Prior checks | N/A |
| Requests from data subjects | 206 585 calls to helpline (includes all calls, i.e. DP, PECR, FOI & EIR; see below for written enquiries and complaints combined). |
| Complaints from data subjects | 26 227 DP cases received (includes written enquiries; includes PECR cases).<br>29 685 DP cases closed. |
| Advice requested by parliament or government | During 2010. It was a relatively quiet year due to the general election and the settling in of a new coalition Government. We advised the Government/Parliament on the following topics:<br>• the ID Documents Bill;<br>• phone hacking (to Home Affairs Select Committee);<br>• IT governance (to Public Administration Committee);<br>• update on our Surveillance Society Report (to Home Affairs Select Committee);<br>• our monitoring of a database of the Serious Organised Crime Agency (SOCA) (to House of Lords Committee);<br>• advice on privacy risks in crime mapping (to Home Office and Police). |
| Other relevant general activity information | 3 BCRs approved |

| | |
|---|---|
| Inspection Activities | |
| Inspections, investigations | Issued 26 audit reports, resulting from inspections of public and private bodies. Eight resulted from organisations agreeing to an audit as part of investigations of a breach of the Act. 97% of recommendations in reports this year were accepted by organisations, and where we re-audited, 92% of our recommendations are being fully or partly carried out. Common areas for improvement include: internal DP policy awareness by staff, relevant DP training for staff, general security, e.g. lack of encryption on portable devices, shared passwords and lack of basic physical security controls, e.g. lockable storage. |
| Sanction Activities | |
| Sanctions | Undertakings: 46<br>Prosecutions: 5<br>Civil Monetary Penalties: 4 |
| Penalties | Civil Monetary Penalties – 4 fines between GBP 60 000 and GBP 100 000 (total GBP 310 000), 3 public sector /1 private sector. These are served by the ICO. |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

### Retention of police records:

In 2008 the Commissioner served Enforcement Notices on five police forces, ordering them to delete old criminal convictions from the police national computer (PNC). This action was taken following our investigation into complaints received from five individuals who had been convicted or cautioned by police on one occasion and had not subsequently been convicted of any other offences.

In each case the Commissioner wrote to the relevant police force and asked for the information to be removed from the PNC, or else 'stepped down'; i.e. retained on the PNC but on the basis that only police users could access the information. Each police force agreed to step down the information, but not to delete it.

As a result the Commissioner served enforcement notices on the Chief Constables of each of the forces. Each notice required the conviction information about the individual in question to be deleted from the PNC.

The Chief Constables appealed to the Information Tribunal, seeking to set aside the Commissioner's enforcement notices. In other words the Chief Constables were seeking to ensure that they could retain the relevant conviction information on the PNC.

The Tribunal upheld the enforcement notices issued by the Commissioner, and required the Chief Constables to delete the relevant information about these 5 individuals.

The five Chief Constables were allowed to appeal to the Court of Appeal, which ruled that the police forces did not need to delete the information and that they had not retained the records in breach of the DPA. The judgment can

be viewed at: www.bailii.org/ew/cases/EWCA/Civ/2009/1079.html. We then applied to the Supreme Court for leave to appeal but in 2010 our application was turned down.

We believe the judgment raises important issues, not just for these and the many other individuals about whom very minor and aged conviction details are held, but also about how the DPA is interpreted in practice. It also raises serious questions about the applicability of Article 8 of the European Convention on Human Rights to conviction data held by the police.

# Chapter Three

# European Union and Community Activities

# 3. European Union and Community Activities

## 3.1. EUROPEAN COMMISSION

### EU Data Protection Day 20108, 28/1/2010

The protection of personal data is a fundamental right within the EU. **'Everyone has the right to the protection of personal data concerning him or her'**, says the Charter of Fundamental Rights of the European Union.

The Commission and the Member States of the Council of Europe celebrated Data Protection Day for the fourth time on 28 January 2010.

This date marks the anniversary of the Council of Europe's Convention 108, the first legally binding international instrument related to data protection.

It represents an opportunity for European citizens to become more aware of personal data protection and of what their rights and responsibilities are in this respect.

On this occasion, European Commission organised a closed Workshop on the theme 'How are data subjects informed about the processing of their data and the exercise of their rights?' More specifically, speeches addressed the following topics: information and rights of data subjects in the medical sector; how can data subjects be the primary actors in defending their own privacy?; privacy and data protection in the workplace; the practice of the European Commission concerning information and rights of data subjects; data protection and privacy rights in the electronic communications sector.

### Stakeholder consultation: meeting on the review of the EU's data protection regulatory framework – 1 July 20109

As a follow-up to the public consultation launched in 2009 on the review of the EU's regulatory framework for data protection, the Commission arranged a series of targeted consultation meetings with a number of key stakeholders.

The purpose of these meetings was to **consult with non-public sector stakeholders on a range of issues pertaining to existing data protection rules, to identify problems and to discuss possible solutions.**

A background paper, containing a series of questions, subdivided into themes and designed to guide and structure discussions at the meeting, is available.

### Public consultation on the future EU-US international agreement10

When developing policy and legislation, the European Commission consults widely with EU citizens and stakeholders through public consultations; therefore a public consultation on the future European Union (EU) – United States of America (US) international agreement on personal data protection and information sharing for law enforcement purposes was available to the public from 28 January 2010 until 12 March 2010. The aim of the consultation was to collect opinions with a view to the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes.

8 http://ec.europa.eu/justice/newsroom/data-protection/events/100128_en.htm

9 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/100128_en.htm

There were 64 responses received for this public consultation from citizens, organisations (registered and not registered) and public authorities.

## 3.2. EUROPEAN COURT OF JUSTICE

### Judgment of the Court (Grand Chamber) of 9 March 2010 – European Commission v Federal Republic of Germany (Case C-518/07)11

The Commission initiated infringement proceedings against Germany which ended in a ruling of the European Court of Justice on 9 March 2010 (C-518/07). The ECJ found that Germany had failed to fulfil its obligations under Article 28 of Directive 95/46/EC and ruled that by making the authorities that monitor processing by non-public bodies and undertakings which compete on the market subject to State scrutiny, Germany failed to correctly transpose the requirement that those authorities perform their functions in 'complete independence'.

The ECJ declared that supervisory authorities must act objectively and impartially and therefore remain free from any external influence, be it direct or indirect, and from all public authorities, not only the ones which are supervised. It was pointed out in the ruling that the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks.

## 3.3. EUROPEAN DATA PROTECTION SUPERVISOR

### A) Summary of activities and news

At the level of the European Union (EU), 2010 saw some major trends and policy opportunities which are driving forward more effective protection of personal data. They include the increasingly visible impact of the Lisbon Treaty which, by providing a strong legal basis for comprehensive data protection in all areas of EU policy, has firmly placed data protection at the heart of the EU policy agenda. It also encompasses the ongoing review of the EU legal data protection framework, which is raising high expectations, particularly in view of the growing importance of data protection in the international arena. Finally, the Stockholm programme and the EU Digital Agenda are both highly significant for privacy and data protection.

The need to increase the efforts to ensure effective data protection can be seen in the EDPS activities over 2010. As regards the EDPS' **supervisory role**, the main highlights include:

- A fundamental change of gear in relation to the enforcement of the Data Protection Regulation in the EU administration in order to ensure a more robust approach to enforcement. The new policy sets forth a number of criteria designed to ensure a proactive, consistent and transparent application of the EDPS' enforcement powers.
- An increase in the scope of EDPS supervision which, since the entry into force of the Lisbon Treaty, applies to all EU institutions and bodies, including areas outside the scope of what used to be Community law.
- The adoption of 55 prior-check opinions relating to processing operations of personal data in the EU administration. These include core business activities, such as the Early Warning

11 OJ C 113 of 01.05.2010, p.3.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:113:0003:0004:EN:PDF

Response System for the exchange of information on communicable diseases, and standard administrative procedures, such as staff evaluation, recruitment and promotions.

- An increase in the complexity of complaints received. In 2010, 94 complaints were received, of which around two thirds were inadmissible because they related to issues at national level. Admissible complaints mainly related to questions of access and rectification, misuse, excessive collection and deletion of data. In 11 cases, the EDPS concluded that data protection rules had been violated.

In his **advisory role**, the EDPS placed special emphasis on:

- The modernisation of the EU legal framework for data protection: the EDPS has consistently recommended an ambitious approach to developing a modern, comprehensive framework for data protection, covering all areas of EU policy and ensuring effective protection in practice.
- The Stockholm Programme and the EU Digital Agenda: these two key policy programmes have great relevance for data protection and are therefore closely monitored as part of the EDPS' advisory role. They also demonstrate that data protection is a crucial element of legitimacy and effectiveness in both these areas.
- A record number of 19 legislative opinions: in 2010, opinions were adopted on a number of subjects including major issues concerning the EU Internal Security Agenda, the EU Counter-Terrorism Strategy, a Global Approach to transfers of PNR data to third countries, Information Management in the Area of Freedom, Security and Justice, 'Privacy by Design' in the Digital Agenda, and finally the ACTA Agreement.

In the **area of cooperation**, the EDPS continued to cooperate closely with the authorities established to exercise joint supervision of EU large-scale IT systems. In particular, important work was done in 'coordinated supervision' of the Eurodac system and the Customs Information System, where the responsibilities for supervision are shared with national colleagues. In cooperation with the European University in Florence, the EDPS also organised a workshop on 'Data Protection in International Organisations' to address the various challenges faced by international organisations when trying to ensure a good level of data protection without a clear legal basis.

| **Organisation** | European Data Protection Supervisor |
|---|---|
| Chair and/or College | Peter Hustinx, Supervisor<br>Giovanni Buttarelli, Assistant Supervisor |
| Budget | EUR 7 104 351 |
| Staff | 38 officials |
| **General Activity** | |
| Decisions, opinions, recommendations | 19 legislative opinions adopted on a number of subjects, including major issues such as the EU Internal Security Agenda, the EU Counter-Terrorism Strategy, a Global Approach to transfers of PNR data to third countries, Information Management in the Area of Freedom, Security and Justice, 'Privacy by Design' in the EU Digital Agenda, and the ACTA Agreement.<br><br>7 sets of formal comments issued on, among other things, the revision |

| | |
|---|---|
| | of the Frontex Regulation, open internet and net neutrality, Internal Market Information System, security scanners, and international data exchange agreements. |
| Notifications | 89 notifications of processing operations presenting specific risks received from EU institutions and bodies' Data Protection Officers for prior checking. |
| Prior checks | 55 prior-check opinions adopted, notably on health data, staff evaluation, recruitment, time management, security investigations, telephone recording and performance tools. |
| Requests from data subjects | 141 requests for information or advice received in writing from the general public. |
| Complaints from data subjects | 94 complaints received, 25 admissible.<br>Main types of alleged violations: violation of confidentiality of data, excessive collection of data or illegal use of data by the controller.<br>10 cases resolved where the EDPS found no breach of data protection rule.<br>11 declared cases of non-compliance with data protection rules. |
| Advice requested by parliament or government | Within the 19 legislative opinions mentioned above, 11 were issued upon request from the European Commission. |
| Other relevant general activity information | 35 consultations on administrative measures related to the processing of personal data in the EU administration. Advice was given on a wide range of legal aspects related to the processing of personal data conducted by EU institutions and bodies. |
| Inspection Activities | |
| Inspections, investigations | On-the-spot inspection carried out in an EU institution.<br>Systematic follow-up of previous inspections and targeted monitoring and reporting exercises, including on-the-spot visits. |
| Sanction Activities | |
| Sanctions | N/A |
| Penalties | Adoption of a new compliance and enforcement policy to ensure a more robust approach to enforcement. The new policy sets forth a number of criteria designed to ensure a proactive, consistent and transparent application of the EDPS' enforcement powers. |
| DPOs | |

| | |
|---|---|
| Figures on DPOs | 47 DPOs in EU institutions and bodies. |

## B. Information on case-law

### Public access to documents containing personal data

Since the start of his activities, the EDPS has continuously dealt with the sometimes complicated relationship between EU rules on public access to documents and EU rules on data protection. The EDPS has first done so by providing guidance to EU institutions, notably with the publication of a Background Paper in 2005.

The EDPS also defended his approach as intervening party in the leading Court case *Bavarian Lager v. Commission*, which concerned a request for public access to the minutes of a Commission meeting, including the names of the participants. Access to those names was refused on the basis of data protection rules. While the General Court agreed with the position advocated by the EDPS, the Court of Justice in appeal, in its judgment of 29 June 2010, overruled the decision of the General Court and gave a different interpretation of the applicable EU rules.

Part of the analysis presented in the Background Paper of 2005 was no longer valid in the light of the Court's judgment. The EDPS therefore prepared an additional paper in which he emphasised the need for a proactive approach to the matter, i.e. institutions should make clear to data subjects – before or at least at the moment they collect their personal data – the extent to which the processing of such data includes or might include its public disclosure. The EDPS took the position that institutions were obliged to do so as a matter of good practice.

Several pending Court cases were suspended, awaiting the *Bavarian Lager* judgment. All these cases were revived after the judgment of the Court in June 2010. The EDPS was an intervener in several of these cases. Where relevant, the EDPS used the opportunity to express his views on the application of the judgment of the Court in *Bavarian Lager* to these other situations. The EDPS has also provided such input in a newly instigated case on the matter.

The *Bavarian Lager* judgment also resulted in, as a consequence, the dismissal of the first case lodged against the EDPS before the General Court.

### Other Court issues

Another judgment with EDPS involvement was delivered by the Civil Service Tribunal on 15 June 2010 in *Pachtitis v Commission*. One of the issues at stake was the refusal of the Commission to provide the applicant with access to the questions of a placement test in which he had participated. Since the data protection rules were invoked in this respect and the matter raised an interesting question about the scope of the right of access to one's own personal data, the EDPS intervened. He did so on the side of the applicant. The applicant won the case, but the data protection issue was not dealt with. For that reason the EDPS withdrew from the subsequent appeal instigated by the Commission before the General Court.

In July 2010, the Civil Service Tribunal invited the EDPS to intervene in a case which concerned the transfer of medical data between two EU institutions. It was the first time that the EDPS has been invited by the Court to intervene in a case. The EDPS accepted the invitation and prepared a statement of intervention in which he clarified the applicable provisions of the Data Protection Regulation.

# Chapter Four
# Principal Developments in EEA Countries

# 4. Principal Developments in EEA Countries

## ICELAND

### A. Summary of activities and news

One of the major issues in 2010 was a draft proposal on new legislation regarding scientific research. The proposal has not yet been presented as a Parliamentary bill, but the Icelandic DPA has given its opinion on key points in the proposal. According to current legislation, access to health records for scientific purposes must be approved by the DPA. According to the draft proposal, however, the DPA's approval will no longer be needed. Instead, bioethics commissions (in most cases the National Bioethics Commission, but in some cases commissions in the largest health care institutions) will evaluate data protection issues when issuing permits for scientific research projects. The DPA has objected to this and has, amongst other things, pointed out that an independent evaluation of legal requirements for access to health records is necessary.

Another major issue was the implementation of new legislation on patient information, i.e. Act No 55/2009 on Health Records. According to this Act, more than one health institution can utilise the same electronic health records information system, given that the minister of welfare approves it and, furthermore, that the DPA confirms that the security of personal data is adequately protected. The DPA gave one such confirmation in 2010, i.e. for a joint electronic health records system for health institutions in Northern Iceland. According to the DPA's decision on the matter, it was a prerequisite for the establishment of the system that there was, amongst other things, logging of all access and an adequate inner audit. Furthermore, the DPA emphasized that provisions in the Act on Health Records on patients' right to prevent access to data must be sufficiently implemented.

In Iceland, each inhabitant is given a unique personal identity number. According to the Data Protection Act, this number shall only be used when necessary to assure correct identification of an individual. The DPA handled a number of cases regarding this number in 2010, including its use by financial institutions. According to legislation on prevention of money laundering and terrorist financing, the correct identification of customers is one of the means by which such activities shall be prevented. However, in line with Directive 2005/60/EC, the application of certain strict measures in that regard is only obligatory when the size of transactions exceeds a certain amount. Still, the DPA received two complaints, according to which customers were asked to give their personal identity number in cases of transactions of trivial amounts, i.e. when paying bills and changing foreign currency into the Icelandic currency. The DPA came to the conclusion that it contravened the aforementioned rule of the Data Protection Act to ask for the personal identity number in these cases. The financial institutions in question were ordered to change their procedures. Later, it came about that one of them had not obeyed this order. Consequently, the DPA decided to issue daily fines if the procedures were not changed. In the wake of that decision, the DPA received clarifications on improvements rendering daily fines unnecessary.

Another issue of interest is the distribution of images from CCTV cameras, showing alleged theft in supermarkets and stores, to those employed there. The DPA received two complaints regarding such distribution in major store chains. In both cases, the complainants suspected that their pictures were kept in stores as warning signs to employees. The DPA found no proof of pictures of these specific individuals being used in this manner, but it turned out that the store chains in question had large collections of images of individuals used for alerting employees. Furthermore, no information was given to these individuals about this use of their pictures. The DPA pointed out that this procedure could lead to people being unjustly labelled as offenders and that a legal basis for the processing was lacking. Consequently, the DPA came to the conclusion that the processing was unlawful and gave orders for it to be stopped.

A number of legal acts were passed in 2010 containing provisions on processing of personal data, including: Act No 12/2010 on a Nordic Arrest Warrant, concerning, amongst other things, its relationship with the European Arrest Warrant and the Schengen cooperation; Act No 42/2010 on Workplace Identification Cards and Supervision in Workplaces, allowing trade unions and employers' unions to make agreements on cards identifying workers in selected branches and, thereby, facilitating the monitoring of rules regarding the labour market; Act No 78/2010, which changes legal acts regarding foreign exchange transactions, including by adding provisions to Act No 87/1992 on Foreign Exchange, allowing the National Bank to collect extensive information on transactions in foreign currency; and Act Nos 100 and 101/2010 on the Debtors' Ombudsman and on Debt Mitigation for

Individuals, containing provisions on, amongst other things, (a) the Ombudsman's powers to collect data on individuals asking the Ombudsman for assistance in making an agreement with creditors on debt mitigation, (b) the individuals' consent for the collection of data, and (c) transmission of the data to creditors.

| | |
|---|---|
| Organisation | |
| Chair and/or College | Sigrún Jóhannesdóttir, Commissioner; Páll Hreinsson, Chairman of the Board of Directors |
| Budget | ISK 66.4 million, i.e. around EUR 415 000 |
| Staff | Four legal counsels, one secretary |
| | |
| General Activity | |
| Opinions, recommendations | Approximately 70 |
| Notifications | 407 |
| Prior checks | 149 processing permits granted |
| Requests from data subjects | Approximately 300 |
| Complaints from data subjects | 135 |
| Advice requested by parliament or government | Approximately 50 |
| Other relevant general activity information | In all, 1 221 new cases registered in 2010 |
| Inspection Activities | |
| Inspections, investigations | 25 |
| Sanction Activities | |
| Sanctions | With the exception of daily fines issued for each day that the DPA's orders are not complied with, the DPA does not have sanction powers. |
| Penalties | In one case, the DPA decided to issue daily fines if certain procedures were not changed, but received clarifications on improvements rendering daily fines unnecessary. |
| DPOs | |
| Figures on DPOs | N/A |

## B. Information on case-law

On 21 October 2010, the Supreme Court of Iceland passed a judgement (case No 13/2010), which touches on an employer's alleged use of a former employee's private e-mail correspondence from his private e-mail address. The case regarded an agreement on payments to the former employee after the termination of his employment. The employer stated that the former employee had broken the agreement by considering applying for a job with a competitor. Consequently, the employer put an end to the payments. The former employee then filed a case against the employer, who in turn presented the aforementioned e-mail correspondence as proof of the former employee's malice.

The Supreme Court, however, came to the conclusion that it could not be verified that the e-mail correspondence was in fact between the former employee and the competitor. In the light of that and other circumstances, the former employee's demand of being paid in accordance with the contract was endorsed.

No demands were made in the case referring to the possible unlawfulness of access to the correspondence. Therefore, no standpoint is taken in the judgement in that regard. However, the case raises questions on the security of private e-mail correspondence.

# LIECHTENSTEIN

## A. Summary of activities and news

### Data retention

As already reported last year, Liechtenstein introduced the retention of traffic data in the Communications Act (Kommunikationsgesetz – KomG)[12] as early as 2006, without any obligation to implement Directive 2006/24/EC.[13] The Data Protection Agency (Datenschutzstelle – DSS) was against the introduction of data retention in Liechtenstein. Nevertheless, the government and state parliament supported an "arrangement of data protection that was friendly to citizens' and fundamental rights" and rules for the express monitoring authority were included in the KomG.[14] The preparation of a corresponding inspection marked the beginning. The precept in Liechtenstein describes the unconditional retention of traffic data despite the strict criteria for the access to such data "as definitely problematic in relation to fundamental rights. Whether it classifies the constitutional court as unconstitutional may also depend essentially on the relevant future foreign fundamental case law".[15] It remains to be seen whether the constitutional court will have an opportunity to adopt a position on this.

### Google Street View

Throughout last year the DSS maintained close contact with Google in relation to the introduction of the "Street View" service, whereby a concrete framework for conducting drives in Liechtenstein was discussed. It focused on all European developments, especially the Article 29 Data Protection Working Party and in particular on Luxembourg, Austria, Germany and Greece, as well as Switzerland. There was also a government notice on the clarifications which needed to be taken into account. The DSS demanded different measures, in particular in relation to the information for the population about the time, the route and the posting of images on the internet. Even the automated blurring of faces and car registration plates was an issue since, precisely in the initial phase of the publication of images, many faces and car number plates were not restricted so were clearly recognisable and identifiable. As far as the DSS is aware there were no street views captured for the Google Street View service in Liechtenstein up to the end of the reporting year.

### Public relations

On the occasion of the European Data Protection Day on 28 January, the DSS, together with the Institute for Economic Information invited Liechtenstein University to a public event on the topic of internet search engines, entitled "Insights into the world of Google & Co: information hunters and data collectors".

In order to reach as wide a section of the population as possible, the DSS uses a variety of channels. Alongside events, seminars, publications and their website, there is also the annual activity report[16] on the key information measures. The website[17] represents an important and low-cost communication instrument. The number of hits shows that this offer is well received. It is therefore continually being improved and expanded. It offers, for instance, tools for self-tests and other assistance on the topic of data protection.

---

12 As part of the most recent revision of the Communications Act, LGBl. 2006 No. 91.

13 Since Directive 2006/24/EC is not (yet) part of the EEA Agreement, no implementation obligation exists.

14 Art. 52 KomG. See also the DSS Activity report for 2010, 1.3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

15 See Hilmar Hoch: Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht (The regulation of state access to telecommunications data in the Communications Act from a constitutional perspective), in LJZ 4 / 2009, p. 103: http://www.juristenzeitung.li/papers/showpdf/LJZ_2009_04.pdf.

16 http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

17 www.dss.llv.li.

| | |
|---|---|
| **Organisation** | |
| Chair and/or College | Dr Philipp Mittelberger |
| Budget | EUR 470 000 |
| Staff | 2.2 Law, 1.0 Technology, 0.8 Administration |
| **General Activity** | |
| Decisions, opinions, recommendations | 26 statements on draft legislation[18]<br>23 approvals of video surveillance systems |
| Notifications | N/A; in total 542 registered data collections |
| Prior checks | N/A |
| Requests from data subjects | 85 |
| Complaints from data subjects | N/A |
| Advice requested by parliament or government | A government notice[19] on Google Street View |
| Other relevant general activity information | Number of questions submitted increased by 20%: 523 requests compared to 431 in 2009[20] |
| **Inspection Activities** | |
| Inspections, investigations | N/A; checks being prepared |
| **Sanction Activities** | |
| Sanctions | N/A |
| Penalties | N/A |
| **DPOs** | |
| Figures on DPOs | N/A |

[18] See DSS Activity report for 2010, 3., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

[19] In line with Art. 30, para. 1 of the Data Protection Law (Datenschutzgesetz – DSG)

[20] See DSS statistics, DSS Activity report for 2010, IV., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf

## B. Information on case-law

Approvals of video surveillance systems

As of 1 July 2009, operation of a video surveillance system in a public area requires permission from the DSS.[21]

Extensive video surveillance: at the end of 2009 the Vaduz region applied to the DSS for approval of the existing video surveillance system in the city centre of Vaduz. There were 15 colour cameras that needed approval which surveyed an area of around 3,000 sq. m. with fixed positions and constant operation except between Monday and Friday from 10 a.m. to 6 p.m.; images were transferred in real time, recording and other editing options were available and images were retained for a period of four days. The DSS rejected the application with an order. This was essentially on the grounds that there was no corresponding proof to show that the video surveillance system in question was necessary and it was therefore viewed as disproportionate. On a subsequent site inspection by the DSS the angles of many cameras were changed, others had their recording durations reduced, and others were switched off and sealed.

A complaint was raised against the DSS order with the Data Protection Commission. In a decision[22] issued last December the Data Protection Commission essentially supported the view of the DSS, but – contrary to the view of the DSS – approved individual cameras. For instance, the Data Protection Commission justified the approval of two cameras at the entrance to the town hall since this public building is also regularly used to host events at which prominent national and foreign visitors may be present. General experience suggests that this area could be potentially dangerous, and as such, proof of concrete incidents, namely an attack on a publicly exposed person, is not necessary. With a view to monitoring the access permissions and guarantees or increases in the safety of visitors to the town hall, a video surveillance system was deemed to be necessary and was therefore classified as admissible. Similarly, in relation to permission requested for the camera at the bus terminal, proof of a concrete incident was not necessary, since general experience of this type of place suggests that "they frequently contain large gatherings of people of various nationalities, which by their very nature are often confused and hence, as experience has shown, they can be associated with an increased security risk".

In relation to the cameras that were switched off or sealed, the Data Protection Commission maintained the legal perspective of the DSS, namely that these represented a disproportionate invasion of privacy and should therefore be dismantled. Passers-by would be under the false impression that surveillance was being conducted, which also contradicts the principles of good faith. The same applies for dummy cameras.

Retention period for video recordings: during this reporting year the DSS granted partial permission for video surveillance systems in only three cases, all of which concerned applications from banking institutions, which requested a retention period of over 30 days. The Data Protection Law (Datenschutzgesetz – DSG) states that data must categorically be erased at least after 30 days if the data is no longer required for fulfilling its purpose or if the protection interests of affected people are infringed upon by longer retention periods.[23] A complaint against the decision was taken to the Data Protection Commission and the complainants requested permission for a retention period until fulfillment of the recording purpose. In its ruling[24], the Data Protection Commission upheld the judgement of the DSS in all three cases, meaning that the 30-day deadline was to be understood as a clear, unconditional absolute maximum deadline for all circumstances and rejected the complaints as unfounded.

---

21 See also the section on Liechtenstein in the 13th annual report of the Article 29 Data Protection Working Party; more details can be found in DSS Activity report for 2009, at 1.5, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2009.pdf.

22 DSK 2010/2; the full ruling, together with further rulings of the DSK can be accessed at: http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm.

23 Art. 6a, para. 7 DSG, LGBl. 2002 No. 55.

24 DSK 2010/4; see: http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm.

## C. Other important information

The DSS sees its role not only as a reactive contact point, but also pursues its performance mandate actively. An example of this was its provoking a government investigation[25] into data streams in the area of social benefits, which was also picked up and supported in the state parliament discussion on the DSS activity report for 2010. The grounds for this was a complaint on the exchange of health data between different authorities. The case made clear how difficult it is to maintain an overview in the tangled web of social benefits and the underlying information exchange. Information is a fundamental prerequisite for the distribution and use of social benefits. The DSS considers that there has been a lack of national investigation about how the various points that distribute economic support are connected to one another and what information is exchanged between individual points. An investigation should give throw greater light on aspects of data protection and should contribute to higher transparency. This would prevent all possible misuse and reduce duplication of effort.

As part of the International Working Group on Data Protection in Telecommunications (IWGDPT) the DSS introduced a discussion principle[26] on the topic of data protection on mobile end devices (mobile telephones, notebooks, etc.). As a result of the small dimensions and low weight of mobile devices, specific data security risks emerge, e.g. manipulation, loss or theft of the data.

[25] In 2005 the government commissioned an "Analysis of the welfare state in Liechenstein", in which 25 social welfare benefits were investigated. The proposed investigation could link into this.

[26] http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf?1292412668.

# NORWAY

## A. Summary of activities and news

The single most important issue during the year was the debate on the Data Retention Directive. It is no surprise to hear that the Inspectorate argued against implementation of the Directive. The topic resulted in the longest debate in the Parliament related to personal data in many years.

Our legal phone and e-mail service handled over 7 300 calls and e-mails, with 17% of the enquiries being related to the topic of data protection at the work place.

In terms of awareness-raising, we continued our campaign 'You Decide' which is translated into several languages. If anyone wants to look into this material, just contact us.

We also participated in making a test to assess vulnerability to identity theft; the test is available on our website. The test is being adopted by other countries as well.

There was a high level of activity by the Government in the health area. There were many proposals on new health registers which the Inspectorate deems negative for personal data protection. Individuals have little or no control over the use of their personal information in these registers.

The Inspectorate produced a revised permit for all Norwegian-based banks in cooperation with the organisation Finance Norway. This accounted for 251 prior checks out of the 357 handled.

During the year, we started a project on social networking sites. The report is available on our website. As part of the work, we inspected four different social networks.

| | |
|---|---|
| Organisation | Datatilsynet – Norwegian Data Inspectorate |
| Chair and/or College | |
| Budget | NOK 32 million (EUR 4 million approximately) |
| Staff | 37 people and 3 project positions |
| General Activity | |
| Opinions, recommendations | N/A |
| Notifications | 3 693 |
| Prior checks | 357 |
| Requests from data subjects | 449 (number of written cases from private individuals) |
| Complaints from data subjects* | Included in the number above |
| Advice requested by parliament or government | 125 |
| Other relevant general activity information | |
| Inspection Activities | |

| | |
|---|---|
| Inspections, investigations | 135<br>• Employment – access control system and access to e-mail: 11<br>• Children and young people: 6<br>• Ticket Communication: 1<br>• Finance – Payment: 2<br>• Insurance – children and life insurance: 5<br>• Health Research: 10<br>• Health: 14<br>• Sports – Doping: 7<br>• Justice – transfer of personal data: 7<br>• Camera surveillance – shopping centres: 44<br>• Municipality: 7<br>• Schengen (SIS): 2<br>• Social networking sites: 4<br>• Telecom: 5<br>• Education: 8<br>• Welfare: 2 |
| **Sanction Activities** | |
| Sanctions | 1 coercive fine due to lack of response to the DPA |
| Penalties | 3 by DPA – total NOK 120 000 |
| **DPOs** | |
| Figures on DPOs | 173 DPOs approved by the DPA |
| Pr. 30.04.2010 | 161 |
| Pr. 31.08.2010 | 168 |
| Pr. 31.12.2010 | 173 |

## B. Information on case-law

These examples of cases taking place in 2010 are just some that we assume will be of interest to our European colleagues.

### Monitoring at the US Embassy

A national TV channel revealed that Norwegian citizens were monitored on behalf of the American Embassy. The Inspectorate engaged in dialogue with the police who investigated the case and recorded our view. The Authority considered that the Embassy should restrict this form of information gathering to a narrow area around the Embassy.

### File-sharing

The Board of Appeal ruled that a law firm should be allowed to hunt file-sharers after the Data Inspectorate had denied the licence application. It is believed there will be legislation in this area soon.

### Control of telecommunication companies' provision of telephone information to the police

The Inspectorate wanted to check what procedures were in place between telecom companies and the police. We also wanted to look at the criteria that must be satisfied for such action to take place. This is both to ensure that it is easy for police to obtain such information, and as preparation for what we assume is coming – the Data Retention Directive.

### Access to employee e-mail

There were a new set of regulations for access to employee e-mail in 2009. In 2010, the Data Inspectorate issued fines to two companies for breaches of these regulations. In the first case, an employer forwarded all email belonging to an employee to his e-mail address without informing the employee, and saved all of the content. In the other case, a substitute was given access to a sick employee's e-mail account, also without informing the employee. The last example is prohibited even when information is given. The Regulation states that personal e-mail accounts are to be treated as personal information.

# Chapter Five

# Members and Observers of the Article 29 Data Protection Working Party

# 5. Members and Observers of the Article 29 Data Protection Working Party

## MEMBERS OF THE ART. 29 DATA PROTECTION WP IN 2010

| Austria | Belgium |
|---|---|
| Mrs. Eva Souhrada-Kirchmayer (from July 2010)<br>Mrs Waltraut Kotschy (till June 2010)<br>Austrian Data Protection Commission<br>(Datenschutzkommission)<br>Hohenstaufengasse 31 - AT - 1014 Wien<br>Tel: +43 1 531 15 / 2525<br>Fax: +43 1 531 15 / 2690<br>E-mail: dsk@dsk.gv.at<br>Website: http://www.dsk.gv.at/ | Mr Willem Debeuckelaere<br>Commission for the protection of privacy<br>(Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer)<br>Rue Haute, 139 - BE - 1000 Bruxelles<br>Tel: +32(0)2/213.85.40<br>Fax : +32(0)2/213.85.65<br>E-mail: commission@privacycommission.be<br>Website: http://www.privacycommission.be/ |
| **Bulgaria** | **Cyprus** |
| Mr Krassimir Dimitrov<br>Commission for Personal Data Protection –CPDP<br>(Комисия за защита на личните данни)<br>15, Acad.Ivan Evstratiev Geshov blvd.<br>BG- 1431 Sofia Tel+359 2 915 3501<br>Fax: +359 2 915 3525<br>E-mail: kzld@government.bg, kzld@cpdp.bg<br>Website: http://www.cdpd.bg | Mrs Panayiota Polychronidou<br>Commissioner for Personal Data Protection<br>(Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>1, Iasonos str.<br>Athanasia Court, 2nd floor - CY - 1082 Nicosia<br>(P.O. Box 23378 - CY - 1682 Nicosia)<br>Tel: +357 22 818 456<br>Fax: +357 22 304 565<br>E-mail: commissioner@dataprotection.gov.cy<br>Website: http://www.dataprotection.gov.cy |
| **Czech Republic** | **Denmark** |
| Mr Igor Nemec<br>Office for Personal Data Protection<br>(Úřad pro ochranu osobních údajů)<br>Pplk. Sochora 27 - CZ - 170 00 Praha 7<br>Tel: +420 234 665 111<br>Fax: +420 234 665 501<br>E-mail: posta@uoou.cz | Mrs Janni Christoffersen<br>Danish Data Protection Agency<br>(Datatilsynet)<br>Borgergade 28, 5th floor - DK - 1300 Koebenhavn K<br>Tel: +45 3319 3200<br>Fax: +45 3319 3218<br>E-mail: dt@datatilsynet.dk |

| | |
|---|---|
| Website: http://www.uoou.cz/ | Website: http://www.datatilsynet.dk |
| **Estonia** | **Finland** |
| - Mr Viljar Peep<br>- Estonian Data Protection Inspectorate<br>(Andmekaitse Inspektsioon)<br>- Väike - Ameerika 19 - EE - 10129 Tallinn<br>Tel: +372 6274 135<br>Fax: +372 6274 137<br>E-mail: info@aki.ee<br>Website: http://www.aki.ee | Mr Reijo Aarnio<br>Office of the Data Protection Ombudsman<br>(Tietosuojavaltuutetun toimisto)<br>Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki<br>(P.O. Box 315)<br>Tel: +358 10 36 166700<br>Fax: +358 10 36 166735<br>E-mail: tietosuoja@om.fi<br>Website: http://www.tietosuoja.fi |
| **France** | **Germany** |
| Mr Alex Türk<br>**Chairman**<br>President of the French Data Protection Authority<br>(Commission Nationale de l'Informatique et des Libertés - CNIL)<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tel: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br><br>Mr Georges de La Loyère<br>French Data Protection Authority<br>(Commission Nationale de l'Informatique et des Libertés - CNIL)<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tel: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br>E-mail: laloyere@cnil.fr<br>Website: http://www.cnil.fr | Mr Peter Schaar<br>The Federal Commissioner for Data Protection and Freedom of Information<br>(Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)<br>Husarenstraße 30 - DE -53117 Bonn<br>Tel: +49 (0) 228 99-7799-0<br>Fax: +49 (0) 228 99-7799-550<br>E-mail: poststelle@bfdi.bund.de<br>Website: http://www.datenschutz.bund.de<br><br>Mr. Alexander Dix<br>(representing the German States / Bundesländer)<br>The Berlin Commissioner for Data Protection and Freedom of Information<br>(Berliner Beauftragter für Datenschutz und Informationsfreiheit)<br>An der Urania 4-10 – DE – 10787 Berlin<br>Tel: +49 30 13 889 0<br>Fax: +49 30 215 50 50<br>E-mail: mailbox@datenschutz-berlin.de<br>Website: http://www.datenschutz-berlin.de |

| Greece | Hungary |
|---|---|
| Mr Christos Yeraris<br>Hellenic Data Protection Authority<br>(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>Kifisias Av. 1-3, PC 115 23<br>Athens - Greece<br>Tel: +30 210 6475608<br>Fax: +30 210 6475789<br>E-mail: christosyeraris@dpa.gr<br>Website: http://www.dpa.gr | Mr András Jóri<br>Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary (Adatvédelmi Biztos)<br>Nador u. 22 - HU - 1051 Budapest<br>Tel:+36 1 475 7186<br>Fax: +36 1 269 3541<br>E-mail: adatved@obh.hu<br>Website: www.adatvedelmibiztos.hu |
| **Ireland** | **Italy** |
| Mr Billy Hawkes<br>Data Protection Commissioner<br>(An Coimisinéir Cosanta Sonraí)<br>Canal House, Station Rd, Portarlington, IE -Co.Laois<br>Tel: +353 57 868 4800<br>Fax:+353 57 868 4757<br>E-mail: info@dataprotection.ie<br>Website: http://www.dataprotection.ie | Mr Francesco Pizzetti<br>Italian Data Protection Authority<br>(Garante per la protezione dei dati personali)<br>Piazza di Monte Citorio, 121 - IT - 00186 Roma<br>Tel: +39 06.69677.1<br>Fax: +39 06.69677.785<br>E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it<br>Website: http://www.garanteprivacy.it |
| **Latvia** | **Lithuania** |
| Mrs Signe Plumina<br>Data State Inspectorate<br>(Datu valsts inspekcija)<br>Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia<br>Tel: +371 6722 31 31<br>Fax: +371 6722 35 56<br>E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv<br>Website: http://www.dvi.gov.lv | Mr Algirdas Kunčinas<br>State Data Protection Inspectorate<br>(Valstybinė duomenų apsaugos inspekcija)<br>A.Juozapaviciaus str. 6 / Slucko str. 2,<br>LT-01102 Vilnius<br>Tel: +370 5 279 14 45<br>Fax: + 370 5 261 94 94<br>E-mail: ada@ada.lt<br>Website: http://www.ada.lt |

| Luxembourg | Malta |
|---|---|
| Mr Gérard Lommel<br>National Commission for Data Protection<br>(Commission nationale pour la Protection des Données - CNPD)<br>41, avenue de la Gare - L - 1611 Luxembourg<br>Tel: +352 26 10 60 -1<br>Fax: +352 26 10 60 – 29<br>E-mail: info@cnpd.lu<br>Website: http://www.cnpd.lu | Mr Joseph Ebejer<br>Information and Data Protection Commissioner<br>Office of the Information and Data Protection Commissioner<br>2, Airways House, High Street, Sliema SLM 1549<br>MALTA<br>Tel: +356 2328 7100<br>Fax: +356 23287198<br>E-mail: joseph.ebejer@gov.mt<br>Website: http://www.idpc.gov.mt |
| **The Netherlands** | **Poland** |
| Mr Jacob Kohnstamm<br>Dutch Data Protection Authority<br>(College Bescherming Persoonsgegevens - CBP)<br>Juliana van Stolberglaan 4-10, P.O Box 93374<br>2509 AJ The Hague<br>Tel: +31 70 8888500<br>Fax: +31 70 8888501<br>E-mail: info@cbpweb.nl<br>Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl | Mr Wojciech Rafał Wiewiórowski<br>Inspector General for Personal Data Protection<br>(Generalny Inspektor Ochrony Danych Osobowych)<br>ul. Stawki 2 - PL - 00193 Warsaw<br>Tel: +48 22 860 7312; +48 22 860 70 81<br>Fax: +48 22 860 73 13<br>E-mail: desiwm@giodo.gov.pl<br>Website: http://www.giodo.gov.pl |
| **Portugal** | **Romania** |
| Mr Luís Novais Lingnau da Silveira<br>National Commission of Data Protection<br>(Comissão Nacional de Protecção de Dados - CNPD)<br>Rua de São Bento, 148, 3º<br>PT - 1 200-821 Lisboa<br>Tel: +351 21 392 84 00<br>Fax: +351 21 397 68 32<br>E-mail: geral@cnpd.pt<br>Website: http://www.cnpd.pt | Mrs Georgeta Basarabescu<br>National Supervisory Authority for Personal Data Processing<br>(Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal)<br>Olari Street no. 32, Sector 2, RO - Bucharest<br>Tel: +40 21 252 5599<br>Fax: +40 21 252 5757<br>E-mail: georgeta.basarabescu@dataprotection.ro<br>international@dataprotection.ro<br>Website: www.dataprotection.ro |
| **Slovakia** | **Slovenia** |
| Mr Gyula Veszelei | Mrs Natasa Pirc Musar |

| | |
|---|---|
| Office for the Personal Data Protection of the Slovak Republic<br>(Úrad na ochranu osobných údajov Slovenskej republiky)<br>Odborárske námestie 3 - SK - 81760 Bratislava 15<br>Tel: +421 2 5023 9418<br>Fax: +421 2 5023 9441<br>E-mail: statny.dozor@pdp.gov.sk<br>Website: http://www.dataprotection.gov.sk | Information Commissioner<br>(Informacijski pooblaščenec)<br>Vošnjakova 1, SI - 1000 Ljubljana<br>Tel: +386 1 230 97 30<br>Fax: +386 1 230 97 78<br>E-mail: gp.ip@ip-rs.si<br>Website: http://www.ip-rs.si |
| **Spain** | **Sweden** |
| Mr José Luis Rodriguez Álvarez<br>Spanish Data Protection Agency<br>(Agencia Española de Protección de Datos)<br>C/ Jorge Juan, 6<br>ES - 28001 Madrid<br>Tel: +34 91 399 6219/20<br>Fax: + +34 91 445 56 99<br>E-mail: director@agpd.es<br>Website: http://www.agpd.es | Mr Göran Gräslund<br>Data Inspection Board<br>(Datainspektionen)<br>Fleminggatan, 14<br>(Box 8114) - SE - 104 20 Stockholm<br>Tel: +46 8 657 61 57<br>Fax: +46 8 652 86 52<br>E-mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se<br>Website: http://www.datainspektionen.se |
| **United Kingdom** | **European Data Protection Supervisor** |
| Mr Christopher Graham<br>Information Commissioner's Office<br>Wycliffe House<br>Water Lane, Wilmslow SK9 5AF GB<br>Tel: +44 1625 545700<br>Fax: +44 1625 524510<br>E-mail: please use the online enquiry form on our website<br>Website: http://www.ico.gov.uk | Mr Peter Hustinx<br>European Data Protection Supervisor - EDPS<br>Postal address: 60, rue Wiertz, BE - 1047 Brussels<br>Office: rue Montoyer, 63, BE - 1047 Brussels<br>Tel: +32 2 283 1900<br>Fax: +32 2 283 1950<br>E-mail: edps@edps.europa.eu<br>Website: http://www.edps.europa.eu |

## OBSERVERS OF THE ART. 29 DATA PROTECTION WORKING PARTY IN 2010

| Iceland | Norway |
|---|---|
| Mrs Sigrun Johannesdottir<br>Data Protection Authority<br>(Persónuvernd)<br>Raudararstigur 10 - IS - 105 Reykjavik<br>Tel: +354 510 9600<br>Fax: +354 510 9606<br>E-mail: postur@personuvernd.is<br>Website: http://www.personuvernd.is | Mr Kim Ellertsen<br>Data Inspectorate<br>(Datatilsynet)<br>P.O.Box 8177 Dep - NO - 0034 Oslo<br>Tel: +47 22 396900<br>Fax: +47 22 422350<br>E-mail: postkasse@datatilsynet.no<br>Website: http://www.datatilsynet.no |
| **Liechtenstein** | **Republic of Croatia** |
| Mr Philipp Mittelberger<br>Data Protection Commissioner<br>Data Protection Office (Datenschutzstelle, DSS)<br><br>Kirchstrasse 8, Postfach 684 – FL -9490 Vaduz<br>Tel: +423 236 6090<br>Fax: +423 236 6099<br>E-mail: info@dss.llv.li<br>Website http://www.dss.llv.li | Mr. Franjo Lacko<br>Director<br><br>Mrs Sanja Vuk<br>Head of department for EU and Legal Affairs<br><br>Croatian Personal Data Protection Agency<br>(Agencija za zaštitu osobnih podataka - AZOP)<br>Republike Austrije 25, 10000 Zagreb<br>Tel. +385 1 4609 000<br>Fax +385 1 4609 099<br>e-mail: azop@azop.hr or info@azop.hr<br>website: http://www.azop.hr/default.asp |
| **The former Yugoslav Republic of Macedonia** | |
| Mr Dimitar Gjeorgjievski<br>Directorate for Personal Data Protection<br>(ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ)<br>Samoilova 10, 1000 Skopje, RM<br>Tel: +389 2 3230 635<br>Fax: +389 2 3230 635<br>E-mail: info@dzlp.mk<br>Website: www.dzlp.mk | |

| Secretariat of the Art. 29 Working Party |
| --- |
| Mrs Marie-Hélène Boulanger<br>Head of unit<br>European Commission<br>Directorate-General Justice<br>Data Protection Unit<br>Office: MO59 02/13 - BE - 1049 Brussels<br>Tel: +32 2 295 12 87<br>Fax: +32 2 299 8094<br>E-mail: Marie-Helene.Boulanger@ec.europa.eu<br>Website: http://ec.europa.eu/justice/data-protection/index_en.htm |

**European Commission - Directorate-General for Justice**
Fourteenth Annual Report of the Article 29 Working Party on Data Protection

Luxembourg: Publications Office of the European Union
2013 — 128 pp. — 21×29.7 cm

ISBN 978-92-79-29769-4
doi: 10.2838/28916

DS-AA-13-001-EN-C
doi: 10.2838/28916

The Working Party has been established by Article 29 of Directive 95/46/EC.
It is the independent EU Advisory Body on the Protection of personal data.
Its tasks are laid down in Article 30 of Directive 95/46/EC and can be summarised as follows:

- To provide expert opinion from Member State level to the Commission on questions of data protection.
- To promote the uniform application of the general principles of the Directive in all Member States through co-operation between data protection supervisory authorities.
- To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data.
- To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data in the European Community.

Publications Office

ISBN 978-92-79-29769-4