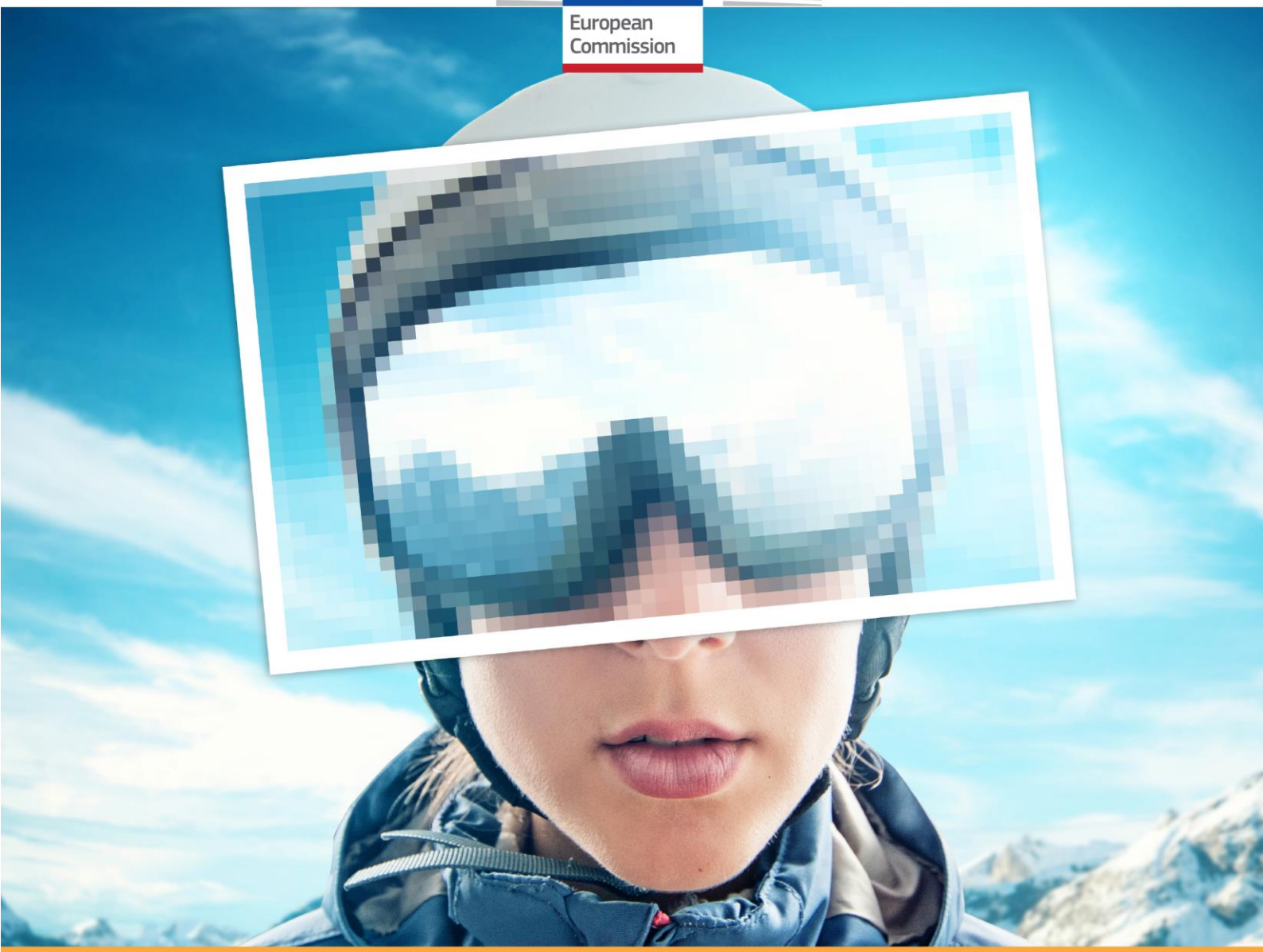
European Commission



Fifteenth Annual Report

of the Article 29 Working Party on Data Protection

Justice and Consumers

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the Internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-79-38255-0
doi: 10.2838/10852
ISSN: 2363-099X

EN

Fifteenth Report of the Article 29 Working Party on Data Protection

Covering the year 2011

Adopted on 3.12.2013

EN

Table of Contents

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

This annual report of the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data provides you with a snapshot of its activities in 2011. The Working Party is an independent advisory body in which all 27 national data protection authorities of the European Union Member States, the European Data Protection Supervisor and the European Commission are represented. The Working Party issues opinions or recommendations on all matters relating to the protection of personal data, contributing to the uniform application and interpretation of the data protection laws in the Member States of the European Union.

In recent years the Working Party has spent much time and effort on the data protection reform process. At the time of writing, the European Commission has already presented the proposals for reforming the data protection rules, consisting of a general Data Protection Regulation and a Directive for the area of criminal law enforcement. The Working Party has always called on the need for comprehensiveness and was therefore slightly disappointed when two different instruments were presented. Nonetheless, comprehensiveness can still be achieved if the instruments provide for the same rights, principles and safeguards. The Working Party has provided input into the reform process and will continue to do so in the future.

Due to the ever-increasing technical possibilities for processing personal data in both the private and public sphere, the protection of an individual's personal data requires all the more attention. A European-wide survey by the Eurobarometer on the attitudes of European citizens on data protection and electronic identity[1] showed that in general individuals do not feel in control when it comes to their personal data.[2]

Since personal data has become the new currency – see for example the shareholders' value of companies that trade in personal data such as Facebook, Google and Twitter – notably this industry seems to be extremely interested in collecting as much personal data from consumers as possible. Often profiles are made of people by organisations in order to personally target them in order to maximise their profits or minimise their risks. The Eurobarometer survey showed, as well as regular contacts between citizens and DPAs, that people are often unaware that their data is being collected. In the event that citizens are aware of the volumes of personal data that is being collected, they feel uncomfortable but do not know how to change it.

This ignorance of citizens concerning the treatment of their own personal data by third parties is the more shocking since data protection is a fundament human right in the EU. It is therefore indisputable that citizens must give their explicit consent to the collection or treatment of their personal data by third parties when there is no other legal ground for these parties to act on. In its opinion on consent the Working Party stressed that only statements or actions, not mere silence or inaction, constitute valid consent. By giving explicit consent, individuals are placed in the driving seat once more when it comes to the processing of their personal data.

The collection of this explicit consent of individuals by the industry is not always respected. In 2011, a new self-regulatory code of conduct on Online Behavioural Advertising (OBA) was developed by the OBA industry. The Working Party examined this framework and concluded that it would not lead to compliance

[1] Eurobarometer, Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union,* June 2011,

[2] The report shows that, on the one hand, 74% of Europeans see disclosing personal information as an increasing part of modern life especially when using the Internet. On the other hand, European citizens do not feel in control when disclosing personal information: just 26% of social network users and 18% of online shoppers feel in complete control. 70% of the citizens are suspicious that companies will use their personal data for purposes other than that for which it was collected.

with European data protection legislation. The Working Party warned that a situation should be avoided in which being compliant with a code of conduct does not lead to compliance with European Privacy law.

Furthermore, the Working Party raised concerns regarding two proposals by the European Commission related to law enforcement access to data held by private companies. The first proposal aimed at setting up a European system allowing law enforcement authorities access to the Passenger Name Records (PNR) registered by airlines for flights arriving in or departing from a Member State. According to the European data protection authorities, the necessity of the proposed system has not been proven. The system as proposed was not privacy friendly and the goals might even be achieved in a different way whereby the privacy law would not be violated.

The Working Party also raised concerns with regard to the proposal to set up a European Terrorist Financial Tracking System (TFTS) which was intended to be a European equivalent of the current United States' TFTP. The programme allows certain law enforcement actors to access information about the international bank transactions carried out in the EU. The data are stored in large databases from which leads regarding the financing of possible terrorist activities can be retrieved by searching the system. The DPAs were not convinced of the necessity or proportionality of the TFTS and made it clear that merely the added value of information derived from the system is not sufficient. In a letter to the European Commission, the Working Party calls upon the Commission to present such evidence, if and when a final proposal is presented.

The earlier mentioned Eurobarometer showed that individuals are worried about the way that their personal data is collected, processed and stored. Therefore it is of the utmost importance that the processing of personal data by private, as well as public organisations is done in accordance with European data protection legislation. The Data Protection Authorities will enforce this law when necessary, both individually and jointly.

Jacob Kohnstamm.

Chapter One
Issues Addressed by the Article 29 Data Protection Working Party[3]

[3]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

1.1 TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1 Passenger Data / PNR

Opinion 10/2011 (WP181) on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

On 2 February 2011 the European Commission published its proposal for a Directive on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The Working Party provided an opinion on the previous EU PNR proposal (Proposal for a Council Framework Decision on the use of passenger name records (PNR) for law enforcement purposes), presented by the Commission on 6 November 2007. The Working Party has also previously commented extensively in several opinions on the various PNR agreements in place between the EU and third countries, and on the Commission's approach as set out in their communication of 21 September 2010. In addition, the Working Party has reiterated its concerns regarding PNR issues in various letters to Commissioner Barrot, Commissioner Malmström, Director-General Faull and the LIBE Committee of the European Parliament.

This opinion is directed at those involved in the discussion and development of the latest proposal, namely the Commission, the GENVAL Council Working Group and the European Parliament.

Conclusion

The Working Party considers that the necessity of an EU PNR system has not yet been proven and the measures proposed are not in line with the proportionality principle, in particular as the system envisages the collection and retention of all data, on all travellers, on all flights. The Working Party also has serious doubts about the proportionality of the systematic matching of all passengers against pre-determined criteria.

The Working Party recommends first evaluating the existing systems and methods of cooperation and how they fit together to identify security gaps. If any exist, then the next step should be to analyse the best way to fill these gaps, which does not necessarily mean introducing a whole new system. The existing mechanisms could be further exploited and improved.

If this proposed Directive comes into force it should ensure appropriate and adequate data protection measures and safeguards. The Commission should also consider whether any existing systems could be repealed as a result, such as the API Directive, to avoid overlapping measures.

1.1.2. Adequacy

Opinion 11/2011 (WP182) on the level of protection of personal data in New Zealand

The Working Party was requested to consider the adequacy of New Zealand data protection legislation in 2009 and the relevant subgroup was given this mandate at the December 2009 plenary.

The European Commission provided a report that it had requested on the adequacy of the protection of personal data in New Zealand, which was written by Professor Roth, Faculty of Law, University of Otago, Dunedin, New Zealand. This report was written under the supervision of the Centre de Recherches

Informatique et Droit (CRID) of the University of Namur. The report analyses the degree to which the New Zealand legal system complies with requirements in terms of substantive legislation and the implementation of mechanisms to apply regulations protecting personal data, 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 Article 29 Working Party on 24 July 1998 (WP 12). It also takes account of non-legal rules, application in practice and the general administrative and corporate culture that exists in relation to privacy.

The subgroup considered this report as well as the comments on this report from the NZ DPA, the NZ Ministry of Justice and the letter from the Ministry of Justice regarding the Privacy (Crossborder Information) Amendment Act 2010. The subgroup also asked the New Zealand Privacy Commissioner (the national supervisory authority) for further information and clarification on some aspects, which are set out below. The subgroup then considered the information received, which included guidance from the Privacy Commissioner on the application of the Privacy (Cross-border Information) Amendment Act following its entry into force on 7 September 2010.

This opinion draws heavily on Professor Roth's report, which was clearly written and helpfully structured to consider New Zealand legislation against each of the requirements in WP 12.

Result of the assessment

New Zealand data protection and privacy law largely predates the EU Directive and implements the OECD guidelines. However, there has been some recent amendments specifically to address concerns about 'adequacy' for transfers of personal data from the EU. The Working Party recalls that although some concerns still exist, adequacy does not mean equivalence with the Directive.

Therefore the Working Party considers that New Zealand 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.

However, the Working Party also encourages the New Zealand authorities to take the necessary steps to address weaknesses in the current legal framework. In particular, the Working Party encourages the Privacy Commissioner to continue her call for strengthening the law in relation to direct marketing; and to maintain effective oversight of transfers from New Zealand to third countries which are not themselves subject to an adequacy finding. The Working Party also requests that, in addition to considering the OECD guidelines and the EU Directive, the Privacy Commissioner also considers relevant European Commission decisions and Article 29 Working Party guidance when deciding whether to issue a transfer prohibition notice.

The Working Party also highlights the fact that, as part of any decision taken by the Commission, it will closely follow the evolution of data protection in New Zealand and the way in which the Office of the Privacy Commissioner applies the principles of data protection referred to in document WP12 and in this document.

1.2. ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 12/2011 (WP183) on smart metering

The objective of the Article 29 Working Party in this opinion is to clarify the legal framework applicable to the operation of smart metering technology within the energy sector. It is not the intention of this opinion to present a comprehensive view on all the specific aspects of smart metering programmes across Member States as the disparity of the current position does not allow us to do so. Smart meters offer new functionalities such as providing detailed information about energy consumption, the ability to remotely read a meter, the development of new tariffs and services based on energy profiles and the ability to remotely deactivate supply.

Smart grids offer even more scope for development and for the processing of more personal data. At this stage the Working Party does not intend to include smart grid functionality in the scope of this opinion. However, we would not rule out further analysis of the smart grid when the picture is clearer.

The EC Directive on Energy End-Use Efficiency and Energy Services (2006/32/EC) sets energy-saving targets to be adopted by each Member State. In order to achieve these targets and, subject to limited exceptions, Article 13 of the Directive obliges Member States to provide consumers with meters that accurately reflect their energy consumption and provide information on actual time of use. These smart meters are part of the attempt to meet the objectives of the European Union related to achieving a sustainable energy supply by 2020.

Conclusions

The arrival of smart metering, which paves the way for the smart grid, brings with it an entirely new and complex model of inter-relationships which poses challenges for the application of data protection law. Responses to the Directorate-General Energy questionnaire demonstrated that there is much diversity in the position across EU Member States, both in terms of progress of the implementation, and energy supply arrangements, which further complicates the scenario. However, what is abundantly clear is that smart metering is enormous in scale: it is projected that the vast majority of European citizens will have one installed in their homes before the end of this decade.

This opinion explains the applicability of data protection law: it has demonstrated that personal data is being processed by the meters, so data protection laws apply. This opinion has shown that smart metering brings with it the potential for numerous novel ways for processing data and delivering services to consumers. Whatever the processing, whether it is similar to that which existed in the pre-smart environment, or unprecedented, the data controller must be clearly identified, and be clear about the obligations arising from data protection legislation including Privacy by Design, security and the rights of the data subject. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that, when they give their consent, it is valid.

Opinion 13/2011 (WP185) on Geolocation services on smart mobile devices

Geographical information plays an important role in our society. Almost all human activities and decisions have a geographical component. In general, the value of information increases when it is connected to a location. All kinds of information can be connected to a geographic location, such as financial data, health data and other consumer behavioural data. With the rapid technological development and wide uptake of smart mobile devices, a whole new category of location-based services is developing.

Chapter One **Issues Addressed by the Article 29 Data Protection Working Party**

The objective of this opinion is to clarify the legal framework applicable to geolocation services that are available on and/or generated by smart mobile devices that can connect with the Internet and are equipped with location sensors such as GPS. Examples of such services are: maps and navigation, geo-personalised services (including nearby points of interest), augmented reality, geotagging of content on the Internet, tracking the whereabouts of friends, child control and location-based advertising.

This opinion also deals with the main three types of infrastructure used to provide geolocation services, namely GPS, GSM base stations and Wi-Fi. Special attention is paid to the new infrastructure based on the location of Wi-Fi access points.

The Working Party is well aware there are many other services that process location data that may also raise data protection concerns. This varies from e-ticketing systems to toll systems for cars and from satellite navigation services, from location tracking with the help of, for example cameras, and the geolocation of IP addresses. However, given the rapid technological developments with regard to especially the mapping of wireless access points, in combination with the fact that new market entrants are preparing to develop new location-based services based on a combination of base station, GPS and Wi-Fi data, the Working Party has decided to specifically clarify the legal requirements for these services under the data protection directive.

The opinion first describes the technology, subsequently identifies and assesses the privacy risks and then provides conclusions about the application of the relevant legal articles to various controllers that collect and process location data derived from mobile devices. This includes, for example, providers of geolocation infrastructure, smartphone manufacturers and the developers of geolocation-based applications.

This opinion will not assess specific geotagging technology linked to the so-called Web 2.0 in which users integrate geo-referenced information on social networks such as Facebook or Twitter. This opinion will also not go into detail about some other geolocation technologies that are used to interconnect devices within a relatively small area (shopping centres, airports, office buildings, etc.) such as Bluetooth, ZigBee, geofencing and Wi-Fi-based RFID tags, though many of the conclusions of this opinion with regard to legitimate grounds, information and data subject rights also apply to these technologies when they are used to geolocate people through their devices.

With the help of geolocation technologies such as base-station data, GPS and mapped Wi-Fi access points, smart mobile devices can be tracked by all kinds of controllers, for purposes ranging from behavioural advertising to child monitoring.

Since smartphones and tablet computers are inextricably linked to their owners, the movement patterns of the devices provide a very intimate insight into the private life of the owners. One of the great risks is that the owners are unaware that they are transmitting their location, and to whom. Another related risk is that the consent for certain applications to use their location data is invalid, because the information about the key elements of the processing is incomprehensible, outdated or otherwise inadequate.

There are different obligations for the different stakeholders, ranging from the developers of the operating systems to application providers and parties such as social networking sites that embed location functionalities for mobile devices in their platforms.

Conclusions

Legal framework

- The EU legal framework for the use of geolocation data from smart mobile devices is primarily the data protection directive. Location data from smart mobile devices are personal data. The combination of the unique MAC address and the calculated location of a Wi-Fi access point should be treated as personal data;

- In addition, the revised E-Privacy Directive 2002/58/EC only applies to the processing of base-station data by telecom operators.

Controllers

- Three types of controllers can be discerned. They are: controllers of geolocation infrastructure (in particular controllers of mapped Wi-Fi access points); providers of geolocation applications and services, and developers of smart mobile device operating system.

Legitimate grounds

- Because location data from smart mobile devices reveal intimate details about the private lives of their owners, the main applicable legitimate ground is prior informed consent;

- Consent cannot be obtained through general terms and conditions;

- Consent must be specific, for the different purposes that data are being processed for, including for example profiling and or behavioural targeting purposes from the controller. If the purposes of the processing change in a material way, the controller must seek renewed specific consent;

- By default, location services must be switched off. A possible opt-out mechanism does not constitute an adequate mechanism to obtain informed user consent;

- Consent is problematic with regard to employees and children. With regard to employees, employers may only adopt this technology when it is demonstrably necessary for a legitimate purpose, and the same goals cannot be achieved with less intrusive means. With regard to children, parents must judge whether the use of such an application is justified in specific circumstances. At the very least they must inform their children, and, as soon as reasonably possible, allow them to participate in the decision to use such an application;

- The Working Party recommends limiting the scope of consent in terms of time and reminds users at least once a year. The Working Party equally recommends sufficient granularity in the consent with regard to the precision of the location data;

- Data subjects must be able to withdraw their consent very simply, without any negative consequences for the use of their device;

- With regard to the mapping of Wi-Fi access points, companies can have a legitimate interest in the necessary collection and processing of the MAC addresses and calculated locations of Wi-Fi access points for the specific purpose of offering geolocation services. The balance of interest between the rights of the controller and the rights of the data subjects requires that the controller offers the right to easily and permanently opt-out of the database, without demanding additional personal data.

Information

- Information must be clear, comprehensive, understandable for a broad, non-technical audience and permanently and easily accessible. The validity of consent is inextricably linked to the quality of the information about the service;

- Third parties, like browsers and social networking sites, have a key role to fulfil when it comes to the visibility and quality of information about the processing of geolocation data.

Data subject rights

- The different controllers of geolocation information from mobile devices should enable their customers to obtain access to their location data in a human readable format and allow for rectification and erasure without collecting excessive personal data;

- Data subjects also have a right to access, rectify and erase possible profiles based on these location data;

- The Working Party recommends the creation of (secure) online access.

Retention periods

- Providers of geolocation applications or services should implement retention policies which ensure that geolocation data, or profiles derived from such data, are deleted after a justified period of time;

- If the developer of the operating system and/or controller of the geolocation infrastructure processes a unique number such as a MAC address or a UDID in relation to location data, the unique identification number may only be stored for a maximum period of 24 hours, for operational purposes.

Opinion 16/2011 (WP188) on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising

In November 2009, the European Parliament and Council adopted Directive 2009/136/EC. This directive revised the 2002 e-Privacy Directive (2002/58/EC). One of the key changes concerns the mechanisms for implanting information in the user's terminal device. The existing opt-out regime, where a user can object to the processing of information collected via terminal equipment (such as 'cookies') was rejected. Instead, the standard became informed consent. These changes play an important role in online behavioural advertising as the industry relies heavily on cookies and similar technologies that store and gain access to information in the user's terminal device.

This requirement for consent reflected a growing concern amongst citizens, politicians, data protection authorities, consumer organisations and policy-makers that the technical possibilities to track individual Internet behaviour over time, across different websites, were rapidly increasing. Furthermore, the possibilities offered to citizens to protect their private life and their personal data against this type of tracking were not keeping pace with this growth. By 2009, policy-makers had strong doubts on the possibility to rely on the relevant advertising industry to increase public awareness and user choice with regard to online behavioural advertising. Many public surveys showed, and continue to show, that the average Internet user is not aware that his/her behaviour is being tracked with the help of cookies or other unique identifiers, by whom or for what purpose. This lack of awareness contrasts sharply with the increasing dependence of many European citizens on access to the Internet for ordinary everyday activities such as shopping, reading, communicating with friends and searching for information. The

Internet is also rapidly replacing several offline activities, such as access to some public services. The rapid replacement of 'fixed' Internet access by mobile access has even further complicated the ability of Internet users to protect themselves with technical means.

Soon after informed consent became the European legal norm, the Article 29 Working Party (hereinafter Article 29 WP) adopted Opinion 2/2010 on Online Behavioural Advertising (OBA)[4] (hereinafter Opinion 2/2010). The opinion describes the roles and responsibilities of the different actors engaged in online behavioural advertising and clarifies the applicable legal framework. The opinion focuses on the tracking of Internet behaviour over time, across different websites as the source of the most important data protection concerns with regard to OBA.

In April 2011 the relevant actors engaged in OBA, represented by both the European Advertising Standards Alliance (EASA) and the Internet Advertising Bureau Europe (IAB), adopted a self-regulatory Best Practice Recommendation on OBA (hereinafter the "EASA/IAB Code")[5]. In August 2011, the Article 29 WP sent an open letter[6] to EASA and IAB outlining the data protection concerns surrounding the opt-out approach suggested within the EASA/IAB Code. In a subsequent meeting with the Article 29 WP, representatives of EASA and IAB stated that "the Code was primarily intended to create a level playing field" and that its purpose was not to achieve compliance with the revised e-Privacy Directive[7].

The Article 29 WP welcomes – as already stated in Opinion 2/2010 – the self-regulatory initiatives of the Industry in the area of behavioural advertising. The EASA/IAB Code indeed includes some interesting approaches (such as Principle V – Education) which can make the consent mechanisms more effective if they are further developed and implemented. However, the EASA/IAB Code per se is not adequate to ensure compliance with the current applicable European data protection legal framework. In order to prevent any misunderstanding, the Article 29 WP has decided to provide specific analysis on the extent to which this Code, as complemented by the website www.youronlinechoices.eu complies with the relevant legal provisions.

More specifically, the current opinion focuses on the first two principles of the EASA/IAB Code and its practical implementation in www.youronlinechoices.eu namely Principle I (Notice) and Principle II (User Choice). In addition, some other principles of the Code, as well as further areas of concern (e.g. data retention) are also discussed. Moreover, the Article 29 WP takes this opportunity to highlight the difference between tracking cookies and other kinds of cookies which may be exempted from consent, providing practical examples of exempted cookies, as well as highlighting possible approaches to legally receive consent where required.

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[5] http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

[6] Letter from the Article 29 Working Party addressed to the Online Behavioural Advertising (OBA) Industry regarding the Self-Regulatory Framework, 3 August 2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

[7] Press release Article 29 Working Party 14 September 2011 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

Conclusions

As stated in its Opinion 2/2010, the Article 29 WP does not question the economic benefits that behavioural advertising may bring, but it firmly believes that such practices must not be carried out at the expense of individuals' rights to privacy and data protection. The EU data protection regulatory framework sets forth specific safeguards which must be respected.

Adherence to the EASA/IAB Code on online behavioural advertising and participation in the website www.youronlinechoices.eu does not result in compliance with the current e-Privacy Directive. Moreover, the Code and the website create the wrong presumption that it is possible to choose not be tracked while surfing the web. This wrong presumption can be damaging to users but also to the industry if they believe that by applying the Code they meet the requirements of the Directive.

The advertising industry needs to comply with the precise requirements of the e-Privacy Directive and this opinion shows that many practical solutions are available to ensure a good level of compliance together with a good user experience.

1.3. RFID

Opinion 9/2011 (WP180) on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

This opinion is a follow-up to Opinion 5/2010 (WP 175) on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. While this introduction will repeat some elements of context necessary to understand the purpose and the scope of this new opinion, the reader is invited to consult Opinion 5/2010 for further details.

On 12 May 2009, the European Commission issued a Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. This Recommendation invited Member States to ensure that the industry, in collaboration with relevant stakeholders, develops a framework for privacy and data protection impact assessment, which was destined to be submitted for endorsement to the Article 29 Data Protection Working Party. Once this framework for privacy and data protection impact assessments is defined, Member States should ensure that RFID operators conduct a privacy and data protection impact assessment (PIA) of RFID applications before they are deployed. Member States should also ensure that the RFID operators will make the resulting PIA Reports available to the competent authority.

On 31 March 2010, industry representatives delivered a Privacy and data protection Impact Assessment Framework proposal to Working Party 29 for endorsement. However, while this proposal presented a good starting point, it didn't gain the full support of the Working Party, notably because of three critical elements that were missing in the proposed framework:

1. A clearly defined risk assessment approach.

2. Consideration for RFID tags carried by persons beyond the operational perimeter of the application.

3. A way to explicitly address the tag deactivation principles in the retail sector that are established in the European Commission's Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

On 13 July 2010, the Working Party summarised these elements, as well as other concerns, in Opinion 5/2010, inviting the industry to propose a revised Privacy and data protection Impact Assessment Framework. With regards to the risk assessment component, the Working Party strongly encouraged the industry to build upon existing expertise that the European Network and Information Security Agency (ENISA) could provide in this area.

During the same month, ENISA published an independent opinion with practical recommendations to improve the proposed Framework. ENISA's opinion proposed in particular some initial guidelines for the adoption of a comprehensive and recognised methodological risk assessment approach, and suggested several structural improvements.

In the following months, the industry redrafted a revised PIA Framework, taking into account the input provided both by the Working Party and ENISA. On 12 January 2011, this revised PIA Framework was submitted for endorsement to the Article 29 Data Protection Working Party.

This opinion formalises the response of the Working Party to this new proposal.

In the following, the RFID Recommendation shall refer to the European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, published on 12 May 2009. The Revised Framework, or simply the Framework, shall refer to the RFID Application Privacy and Data Protection Impact Assessment Framework, transmitted to Working Party 29 on 12 January 2011 and reproduced in the Appendix of this Opinion.

Conclusions

The Working Party endorses the Revised Framework submitted on 12 January 2011. This framework shall take effect no later than six months after the publication of this Opinion.

A PIA is a tool designed to promote "privacy by design", better information to individuals as well as transparency and dialogue with competent authorities. Consequently, since some RFID Applications will be implemented in several Member States, it is important that PIA reports are translated and made available to competent authorities in their national language.

The Working Party will continue to support future dialogue with the industry, with regard to providing enhancements and clarifications in the structure and implementation of the RFID PIA Framework, as informed by experience and feedback from all stakeholders.

1.4. PERSONAL DATA

Opinion 14/2011 (WP186) on data protection issues related to the prevention of money laundering and terrorist financing

The Article 29 Data Protection Working Party ("Working Party") has issued 44 recommendations concerning privacy and data protection related to the prevention of money laundering and terrorist financing (AML/CFT), attached in the Annex to this opinion.

The Working Party 29 will follow up the attached recommendations and the relevant developments in legislation and practice in the combined area of the prevention of money laundering and terrorist financing as well as privacy and data protection.

Opinion 15/2011 (WP187) Consent

The Opinion provides a thorough analysis of the concept of consent as currently used in the Data Protection Directive and in the e-Privacy Directive. Drawing on the experience of the members of the Article 29 Working Party, the Opinion provides numerous examples of valid and invalid consent, focusing on its key elements such as the meaning of "indication", "freely given", "specific", "unambiguous", "explicit" and "informed" etc. The Opinion further clarifies some aspects related to the notion of consent. For example, the timing as to when consent must be obtained, how the right to object differs from consent, etc.

Consent is one of several legal grounds to process personal data. It has an important role, but this does not exclude the possibility, depending on the context, of other legal grounds perhaps being more appropriate from both the controller's and from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his/her data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

This Opinion is partly issued in response to a request from the Commission in the context of the ongoing review of the Data Protection Directive. It therefore contains recommendations for consideration in the review. Those recommendations include:

i. Clarifying the meaning of "unambiguous" consent and explaining that only consent that is based on statements or actions to signify agreement constitutes valid consent.

ii. Requiring data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation).

iii. Adding an explicit requirement regarding the quality and accessibility of the information forming the basis for consent; and

iv. A number of suggestions regarding minors and others lacking legal capacity.

Overall assessment

The Working Party considers that the current data protection framework contains a well-thought out set of rules that establish the conditions for consent to be valid in order to legitimise data processing operations. These apply in both the off- and online environments. More particularly:

The framework successfully achieves the balancing of a number of concerns. On the one hand, it ensures that only true, informed, consent is deemed as such. In this regard, Article 2(h) explicitly requiring consent to be freely given, specific and informed, is relevant and satisfactory. On the other hand, this requirement is not a straight-jacket but it rather provides sufficient flexibility, avoiding technologically specific rules. This is illustrated in the same Article 2(h) where it defines consent as any indication of the individual's wishes. This provides sufficient leeway in terms of the ways in which such an indication can be provided. Articles 7 and 8, requiring respectively unambiguous and explicit consent, capture well the need for a balance between the two concerns, giving flexibility and avoiding overly rigid structures while guaranteeing protection.

The result is a framework which, if properly applied and implemented, is capable of keeping pace with the wide variety of data-processing operations that often result from technological developments.

In practice however, establishing when consent is needed and more particularly the requirements for valid consent, including how to apply them concretely, is not always easy because of a lack of uniformity across Member States. Implementation at national level has resulted in different approaches. More specific shortcomings were identified during the discussions in the Article 29 Working Party that led to this Opinion, further described below.

Possible changes

- The notion of unambiguous consent is helpful for setting up a system that is not overly rigid but provides strong protection. While it has the potential to lead to a reasonable system, unfortunately, its meaning is often misunderstood or simply ignored. While the indications and examples developed above should contribute to enhancing the legal certainty and protection of individuals' rights when consent is used as a legal basis, the above situation seems to call for some amendments;

- More particularly, the Article 29 Working Party considers that the wording itself ("unambiguous") would benefit from further clarification as a part of the revision of the general data protection framework. Clarification should aim at emphasising that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the online environment;

- In addition to the clarification described above, the Article 29 Working Party suggests the following:

  i. *First*, include in the definition of consent of Article 2(h) the word "unambiguous" (or equivalent) in order to reinforce the notion that only consent that is based on statements or actions to signify agreement constitutes valid consent. In addition to adding clarity, this would align the concept of consent under Article 2(h) with the requirements for valid consent under Article 7. Moreover, the meaning of the word "unambiguous" could be further explained in a recital of the future legal framework.

  ii. *Second*, in the context of a general accountability obligation, the controllers should be in a position to demonstrate that consent has been obtained. Indeed, if the burden of proof is reinforced so that data controllers are required to demonstrate that they have effectively obtained the consent of the data subject, they will be compelled to put in place standard practices and mechanisms to seek and prove unambiguous consent. The type of mechanisms will depend on the context and should take into account the facts and circumstances of the processing, more particularly its risks.

- The Article 29 Working Party is not convinced that the legal framework should require explicit consent as a general rule for all types of processing operations, including those currently covered by Article 7 of the Directive. It considers that unambiguous consent which encompasses explicit consent but also consent resulting from unambiguous *actions* should remain the required standard. This choice gives more flexibility to data controllers to collect consent and the overall procedure may be quicker and more user-friendly;

- Several aspects of the legal framework that apply to consent are deduced from the wording, legal history or have been developed through case-law and Article 29 Working Party Opinions. It would provide more legal certainty if such aspects were expressly built in the new data protection legislative framework. The following points could be taken into account:

  i. The inclusion of an express clause setting up the right of individuals to withdraw their consent.

ii. The reinforcement of the notion that consent must be given before the processing starts, or before any further use of the data for purposes not covered by an initial consent, where there is no other legal ground for the processing.

iii. The inclusion of explicit requirements regarding the quality (obligation to provide information on data processing in a manner which is easy to understand, in clear and plain language) and accessibility of the information (obligation for the information to be conspicuous, prominent and directly accessible). This is vital for enabling individuals to make informed decisions.

- Finally, with regard to individuals lacking legal capacity, provisions ensuring enhanced protection could be foreseen, including:

i. Clarifications as to the circumstances in which consent is required from parents or representatives of an incapable individual, including the age threshold below which such consent would be mandatory.

ii. Laying down the obligation to use age-verification mechanisms, which may vary depending on circumstances such as the age of the children, the type of processing, whether particularly risky, and whether the information will be kept by the data controller or made available to third parties.

iii. A requirement for information to be adapted to children insofar as this would make it easier for children to understand what it means when data from them are collected, and thus deliver consent.

iv. Specific safeguards identifying data processing activities, such as behavioural advertising, where consent should not be a possible basis to legitimise the processing of personal data.

The Article 29 Working Party will revisit the issue of consent. More particularly, national data protection authorities as well as the Working Party may decide at a later stage to draft guidelines to develop this Opinion further, providing additional practical examples related to the use of consent.

Working Document 01/2011 (WP184) on the current EU personal data breach framework and recommendations for future policy developments

This Article 29 Working Party document takes stock of the status and the way in which Member States are transposing the personal data breach provisions of the ePrivacy Directive in their national laws[8].

The aim of this exercise is threefold:

First, the Article 29 Working Party wishes to obtain a broad understanding of the current situation on this topic. This includes both basic aspects, such as the status of transposition, and more complex ones, for example, identifying any initial differences of approach in different areas (e.g. the scope of the obligation, whether national guidance developing some aspects of the ePrivacy Directive is foreseen, the national competent authority, etc.). Pinpointing any developing differing national approaches might, even at this late stage, enable Member States to align their views and avoid fragmented implementation.

[8] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L337/11, 18.12.2009.

Second, this activity is helping national data protection authorities to take note of the findings and it has brought to their attention the need to engage in some follow-up activities, described in this working paper. It emerges from this activity that competent authorities ought to continue working towards defining internal rules and procedures for data controllers to notify individuals and competent authorities. Furthermore, taking into account that data controllers will be increasingly notifying cross-border personal data breaches, the need for authorities to liaise to discuss a cooperation method becomes obvious.

In addition, this exercise has given the Article 29 Working Party an opportunity to further reflect on the matter and reach some conclusions as to future policy developments in the area of personal data breach notification. These conclusions, which complement the views of Article 29 Working Party on the topic given on other occasions[9], build on the experience of security breach notification that has been gained by those national data protection authorities already implementing personal data breach notification requirements. The Article 29 Working Party wishes that these findings are taken into account in the context of further policy developments regarding personal data breaches. More particularly, such policy developments are expected in the following two contexts:

a) To complement the personal data breach framework of the ePrivacy Directive. Article 4(5) of the ePrivacy Directive delegates powers to the Commission to adopt technical implementing measures (referred to as "delegated powers" *ex* Article 290 of TFEU, after the adoption of the Lisbon Treaty) in order to ensure consistent implementation and application of the personal data breach legal framework in some well-defined areas, (i.e. circumstances, format and procedures applicable to the information and notification requirements).

b) To extend the personal data breach framework of the ePrivacy Directive in the context of the review of Directive 95/46. The Commission committed before the European Parliament to initiate without delay the appropriate preparatory work, including consultation with stakeholders, with a view to presenting proposals in this area, as appropriate, by the end of 2011...[10]. This commitment was confirmed in the Commission's Communication, A comprehensive approach on personal data protection in the European Union[11].

The above items are developed as follows: After a summary of the main elements of the personal data breach provisions in the ePrivacy Directive (Section II), this working document summarises the personal data breach legislation in Member States (Section III). The summary is based on information provided by the national data protection authorities (DPAs) but not reproduced here given the evolving character of the transposition. Section IV puts forward various actions to be carried out by competent authorities and by the Article 29 Working Party towards developing internal processes and setting forth cooperation procedures. Section V and VI focus on the new policy developments by recalling the overall scope and procedures for the expected policy actions regarding personal data breach and providing policy recommendations.

The views expressed here are without prejudice to possible more specific guidance in the future, including in the context of the adoption by the Commission of technical implementing measures *ex* Article 4(5) of the ePrivacy Directive.

---

[9] See WP 29 Paper entitled, "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", adopted on 1.12.2009 (WP 168); Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), adopted on 10.2.2009 (WP 159); Opinion 2/2008 on the review of Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), adopted on 15.5.2008 (WP 150).

[10] See Commission declaration on data breach notification made before the European Parliament in 2009 in the context of the reform of the Regulatory Framework for Electronic Communications. Retrievable at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-ta-2009-

[11] COM(2010) 609 final, adopted on 4.11.2010.

Chapter Two

Main Developments in Member States

AUSTRIA

A. New developments and activities

In the reporting period, the government bill for an **amendment to Administrative Jurisdiction Act [Verwaltungsgerichtsbarkeits-Novelle] 2012** was adopted.[12] This amendment provides that certain independent administrative authorities (including the Data Protection Commission) will be dissolved as at the end of 2013, with their judicial activities transferring to newly created administrative courts. The Data Protection Commission has repeatedly criticised the proposal to dissolve it. If the Data Protection Commission is dissolved, a new Data Protection Authority will have to be established on the basis of Article 28 of Directive 95/46/EC, to which the tasks of the Data Protection Commission will be transferred. The original idea of transferring formal legal decisions to an administrative court appears problematic, both with regard to the 'effective powers of intervention' mentioned in Article 28 of Directive 95/46/EC, and also to the trend that can be seen in the draft of a 'General Data Protection Regulation' to strengthen data protection authorities and to standardise the competences of the European data protection authorities. This could involve a legal process passing from the data protection authority to an administrative court.

In the reporting period, the bill for an '**Electronic Health Records Act'** [ELGA-G] was issued by the Federal Ministry of Health, to which the Data Protection Commission has submitted a detailed response.[13] Working document WP 131 from the Article 29 working party on the processing of personal data relating to health in electronic health records (EHR) from 2007 played a significant role in the drafting of the bill. The bill subsequently underwent numerous revisions.[14]

In the reporting period the Data Protection Commission cooperated in a **data protection twinning project in Montenegro**. One purpose of EU twinning projects is to share the expertise of established authorities on the creation and expansion of public structures in countries which are or will be accession candidates. In this case, members of the Data Protection Commission and staff from its office shared their expertise within the framework of short term projects. The chief executive of the Data Protection Commission also assumed the role of project manager for Austria in the last months of the project. In 2011, a study visit was made by representatives of the Montenegrin data protection authority to the Data Protection Commission in Vienna.

For **European Data Protection Day 2011**, an event was held together with the Data Protection Council and the Federal Chancellery – something which has already become a tradition – dedicated primarily to the future of data protection in the internet age. A particular topic at this event was also the strategy of the European Commission for a new legal data protection framework.

[12] It has now been passed by the National Assembly and Federal Council and published in the Federal Law Gazette (BGBl.) I 51/2012.

[13] see http://www.dsk.gv.at/DocView.axd?CobId=42793

[14] The government bill for an 'Electronic Health Records Act' was passed in October 2012.

Organisation	Austrian Data Protection Commission
Chair and/or College	Chair: Dr Anton SPENLING Executive member: Dr Eva SOUHRADA-KIRCHMAYER 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	84 formal decisions (complaints), 220 Ombudsman cases, 43 authorisations (data transfer in third countries, research and surveys), 155 formal decisions in the notification procedure and 3 formal recommendations.
Notifications	12 542
Prior checks	2 167
Requests from data subjects	Writing: 1 327 Phone: approx. 25 000
Complaints from data subjects	Complaints leading to a formal decision: 84
Advice requested by parliament or government	Complaints leading to a clarification or recommendation: 220
Other relevant general activity information	This falls into the competence of two other institutions: the "Datenschutzrat" (data protection council) and the legal service of the Government in the Federal Chancellery).
Inspection Activities	
Inspections, investigations	13. Most of the cases are related to video surveillance.
Sanction Activities	
Sanctions	None. The Austrian DPA cannot 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

In the reporting year, the registration procedure for **Google Street View**, which was rolled out in 2010, was completed. The Data Protection Commission approved the registration of Google Street View and also issued three recommendations to Google Inc. The excerpt from the register and the recommendations were sent to Google Inc. on 21 April 2011. The registration concluded the procedure for determining the main facts relating to the 'Google Street View' application registered by Google Inc. (application for cartography purposes and for publication in 'Google Street View'). In this process, Google Inc. made the requested improvements to the registration.

In addition to the commitments already made by Google Inc. during the registration and the audit process (e.g. to conceal faces and car registration numbers before publishing the data on the internet, and to provide information to the public), the following recommendations were made to Google Inc.:

a) If persons are photographed in particularly sensitive areas, not only the faces but also the entire images of the persons must be made unrecognisable. This includes, in particular, entrance areas to churches and other places of worship, hospitals, women's shelters and prisons.

b) Photographs of private property not visible to pedestrians, such as fenced private gardens and yards, must be concealed before publication on the internet.

c) According to Section 28(2) of the Data Protection Act [DSG] 2000, the data subject is entitled to a right to object from the time the data is gathered. In order to allow the data subject to object to publication of buildings even before publication of the image data, appropriate tools must be provided which facilitate a simple and non-bureaucratic assertion of the right to object. The right of objection (even before publication) and the tool for exercising the right of objection also has to be referred to on the website of Google Inc.

Recommendations a) and b) must be implemented by the time of publication of the data on the internet at the latest. The tool and the reference to it according to recommendation c) must be in place at least twelve weeks before publication of data on the internet.

Google has not so far placed the Street View data it has previously collected on the internet. As far as can be determined, there were no other Street View journeys in Austria.

In a complaint, the Data Protection Commission discussed the **identity check when exercising the right to information**. An information requestor, who has already proven his identity by sending a copy of his ID card and a facsimile of his signature (in addition to the signed request for information), had been required by the client also to provide the forenames of his parents in order to obtain the requested information. The Data Protection Commission considered the proof of identity already provided to be sufficient. By insisting on being provided with the forenames of the complainant's parents and by not providing the data protection information, despite the proof of identity provided, it breached the complainant's right to information about his own data.

BELGIUM

A. Summary of the activities and news

Cybersurveillance in the workplace

The control of internet and email use in the workplace has been an ongoing issue for the Privacy Commission (CPP) in recent years. It regularly received questions, complaints and requests for recommendations and guidelines to follow for defining a company policy that is both legal and practicable.
The CPP therefore took the initiative to issue a statement on these questions, first of all by publishing an in-depth analysis report on the subject in 2011, a kind of green paper containing information used as the basis for a series of practical recommendations published, following an extensive public enquiry, in May 2012. This report can be found on the Privacy Commission website:
http://www.privacycommission.be/fr/brochure-information-cybersurveillance
In this report, the CPP states that these controls have a legal basis in the authority under which the employee carries out his or her work on behalf of the employer to which he or she is bound by an employment contract (contractual subordination). Within the context of the employment contract, the worker communicates electronically with third parties, using the IT system provided by the employer to do so. The results of any work that is done, performed using IT tools, including the internet and the employer's email system, must of course be provided to the employer. The employer should be able to receive this information from the individual in question or should be able to look for and find it in order to ensure the continuity of service and correct functioning of the company, in particular in the event of absence, death or departure of the worker from the company.
These checks must nonetheless be performed pursuant to the applicable legal provisions, including the *Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (Privacy Law).* Notwithstanding these requirements, the employer must be and remain able to effectively protect its lawful interests (management and organisation of its activities).

Greater transparency in marketing surveys

As had already been done several times in the past, the marketing department of the Belgian Post Group (Bpost) launched an extensive survey of millions of Belgian citizens in 2011. Bpost wanted to establish a profile for its customers in order to carry out direct marketing. The data is sold to companies who then send out targeted advertising. The Belgian Post Group advertising survey was deemed by the CPP to be aggressive and not sufficiently transparent, perhaps even misleading. For example, Bpost did not state clearly that it was not mandatory to fill in this purely marketing survey. The survey was also sent in a brown envelope, very similar to the one used for sending tax declarations, and during the very period in which these declarations are sent. Alerted by the general public, in particular by elderly people who felt pressured by the nature of this questionnaire, the CPP began negotiations with the Belgian Post Group, who allowed a more transparent questionnaire and clearer information to be established in line with everybody's lawful interests.
For everything else, all of the CPP's activities are covered in its 2011 Annual Report available at:
http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2011.pdf

Organisation	
Chair and/or College	Name of the chair, if applicable composition of the college. Chairman: W. Debeuckelaere (magistrate) Vice-Chairman: S. Verschuere College members: M. Salmon (Court of Appeal advisor), S. Mertens de Wilmars (teacher), A. Vander Donckt (notary), F. Robben (general manager of the Banque Carrefour de la Sécurité Sociale and the e-health platform), P. Poma (magistrate), A. Junion (lawyer). For the deputy members, visit the Privacy Commission website: (http://www.privacycommission.be) and read the 2011 Annual Report. See also Article 24, section 4, paragraphs 3 and 4: *"The Commission is formed in such a way that an equilibrium exists between the different socioeconomic groups. In addition to the Chairman, the Commission includes, amongst its actual members and its deputy members, at least the following: a legal expert, an IT specialist, a person with proven professional experience of managing personal data in the private sector and a person with proven professional experience of managing personal data in the public sector".*
Budget	Budget allocated and executed. Budget allocated: EUR 5 516 000 (2011) / EUR 5 684 000 (2012)
Staff	Number of staff (if applicable by field of employment): 52 employees. (1 Chairman – 1 Vice-Chairman). Heads of section: 3 Personnel and Organisation (20): accounts (1), translators (5), administration (8), statistics (1), personnel manager (1), logistics (2), IT support (1), communication manager (1). Studies and Research (18) legal counsel (16), IT specialist (1), research assistant (1). External relations (Front Office) (11): legal counsel (4), assistants (7).
General Activity	
Decisions, opinions, recommendations	Number of opinions and key topics, here we should count any text produced by the DPA having an effect on data protection in general, on data subjects or on data controllers.

	Opinions (upon request from the legislative or executive power - see below): 29 Opinions and initiative recommendations: 14 Recommendations within the context of further processing declarations: 10
Notifications	Number of notifications, if applicable, as per the definition provided by the national legislation. In 2011, the processing managers entered 7,169 declaration files via the electronic access point, which represents a 92% increase compared to the number of declaration files entered in 2010. In 2011, 6,490 new data processing operations were declared: • Ordinary declaration (19%); • Declaration via DPR (subscription to a declaration entered by an "umbrella" body for example); • Declaration of further processing (1%); • Thematic declaration for the installation and use of a surveillance camera (52%). 372 declarations of amendments to processing operations already made. 124 declaration corrections. 306 end-of-processing declarations. The main aims of the processes declared were: "surveillance and inspection" (2,850); "surveillance and inspection of people working in a monitored workplace" (520); "general purposes" (542), "healthcare" (104), "other" (2,043).
Prior checks	If applicable, number of prior checks, understood as per the definition provided by the national legislation. Even if the authorisation activity of the sector committees does not reflect the subject of Article 20 of Directive 95/46/EC exactly, the different sector committees established within the Commission have returned the following number of authorisations: • Federal authority sector committee: 108 (individual and subscriptions to general authorisations); • Statistics sector committee: 35 (individual);

	• National Register sector committee: 286 (individual and subscriptions to general authorisations). Social security and healthcare sector committee: • Healthcare section: opinions (1) – deliberations (34); • Social security section: opinions (23) – deliberations (87).
Requests from data subjects	Number of requests received in writing or by phone if applicable, from data subjects The statistics of the Belgian Privacy Commission do not make any distinction between requests for information from data subjects and those from data controllers: Information given by the Front Office: 3,042 "Questions & Answers" files opened in 2011 (publicity right, principles of protection of privacy, economy/consumer credit, privacy in the workplace and public authorities. The CPP also handled 2,866 requests for information or mediation (including inspection files): These files can be broken down as follows: 2,447 requests for information both from public bodies and current or future data controllers and from data subjects, 296 requests for mediation and 123 inspection files.
Complaints from data subjects	Number of qualified complaints (if relevant by type): See above: 296 requests for mediation: before any mediation or communication of information, the CPP always analyses admissibility. For 153 files, the request for mediation was found to be inadmissible, often due to a lack of information from the data subject (148 files). 215 requests (9%) were sent in error to the Privacy Commission, which always endeavoured to point the applicant in the direction of the competent institution. In almost 75% of cases, the CPP was successful. In 75% of the questions handled, information relating to privacy was communicated. In 3.85% of files, the complaint proved to be unfounded. On the other hand, in 5.01% of files, a breach of privacy was found and a correction obtained.
Advice requested by parliament or government	Any text document produced at the request of the parliament or government or produced at the intention of the government: A list of the opinions issued by the Belgian Commission in 2011 is available on its website at: http://www.privacycommission.be
Other relevant general activity information	Number of "relevant number to be chosen by DPAs" Any relevant figures reflecting the activity of the DPA, for instance

	number of BCRs approved as a lead DPA. See the Annual Report of the Belgian Privacy Commission, which contains an extensive and detailed "statistics" section. This Annual Report is available from the Commission's website: http://www.privacycommission.be
Inspection activities	
Inspections, investigations	Number of inspections and/or investigations (by key topics if available); if applicable, as per the national legislation. 123 inspections (see below). The topics most frequently covered (information, mediation/complaint and inspections) are as follows: Handling of images including video surveillance in particular Principles of protection of privacy Processing of data by public authorities Commercial practices (primarily marketing)

Sanction activities	
Sanctions	Numbers of sanctions decided by the DPA (if provided by national law). Number of legal actions started by the DPA against data controllers (if provided by national law). The CPP does not have its own sanction authority. However, it can send files in which it has found breaches to the Public Prosecutor's office.
Penalties	Amounts (indication on whether imposed by courts or DPAs): The CPP does not have its own sanction authority. However, it can send files in which it has found breaches to the Public Prosecutor's office.
DPOs	
Figures on DPOs	Diverse figures are admissible depending on information available in Member States. If not provided by national law, the cell shall be marked with N/A. The CPP does not have this information.

B. Information on case-law

Google prosecuted by the Public Prosecutor's office as a result of the Google Street View Wi-Fi incident

The CPP is not authorised to issue fines to data controllers who breach the "Privacy Law". Nonetheless, it has a duty to report to the Public Prosecutor's office any offences of which it learns. With regard to the Google Street View Wi-Fi incident or the capture of personal Wi-Fi data (network name, URL, whole emails and sometimes also passwords) through unprotected networks by "Google cars" fitted out to take panoramic photographs in order to populate Google Street View, the CPP contacted the federal Public Prosecutor's office. Google has acknowledged its mistake and accepted the proposal of the Belgian Public Prosecutor's office to pay the sum of €150,000.

BULGARIA

A. Summary of the activities and news

Organisation	
Chair and/or College	Commission for Personal Data Protection (CPDP) with Chair – Mrs Veneta Shopova, and four members – Mr Krassimir Dimitrov, Mr Valentin Enev, Mrs Mariya Mateva and Mr Veselin Tselkov.
Budget	Allocated budget – BGN 2 560 000 (Bulgarian currency), executed budget – BGN 2 344 993.
Staff	Number of employees – 76
General activity	
Decisions, opinions, recommendations	In 2011 203 decisions were issued, of which 50 were opinions and 30 compulsory instructions, primarily affecting parties to administrative procedures. In addition, the period between their issuing and taking effect was too short for the data controller to take into account the CPDP's recommendations and to change and improve its work with regard to individuals' personal data protection. Parts of the acts were appealed before the court and the hearings are currently continuing, which delays their coming into force.
Notifications	42 911 personal data controllers.
Prior checks	1 151
Requests from data subjects	In total 458 requests, complaints and notifications, 102 of which were requests and 15 complaints. From the received requests most allegations of violations of rights under the Law for Protection of Personal Data (LPPD) were in the fields of: telecommunications (15), Internet (12), state administration (11), trade and services (10). Visibly lesser are the statements in the financial sector (5), media (2), healthcare (2) and political parties (2).
Complaints from data subjects	341 – in fields including: telecommunication and information society – 199; media – 8; healthcare – 5; banks and banking institutions – 27; insurance services – 11.
Advice requested by parliament or government	Three Opinions on the elections for President and Vice-President of the Republic of Bulgaria and for municipal councils and mayors in 2011; Two Opinions on requests for the provision of access to personal data in NSIS and on the maintaining of the public donations register by the Ministry of the Interior and the possibility

	to publish the personal data of donors, who are individuals; Three Opinions on requests by the Ministry of Foreign Affairs about the lawfulness of processing personal data and their transfer to foreign state authorities, and about the policy for facilitating the procedure for providing administrative services to Bulgarian citizens abroad when they receive Bulgarian identification documents.
Other relevant general activity information	With regard to transfers of personal data transfers, the Law for the Protection of Personal Data foresees an authorisation regime, and, for the reporting period, 21 requests for authorisation of transfers of personal data to third countries were dealt with. With regard to binding corporate rules, the CPDP approves lead authority and co-ordinates documents on the approval of corporate rules under the mutual recognition procedure and in 2011, nine requests for approval were entered.
Inspection activities	
Inspections, investigations	In 2011 the total number of inspections conducted was 1 252, of which: *ex-ante* – 1 151; ongoing – 74 and *ex-post* – 27, mainly in the fields of: healthcare – 612; trade and services – 153; tourism – 57; legal and consultants services – 53; transport – 47; state administration – 46; social activities – 40 etc.
Sanction activities	
Sanctions	In 2011, the CPDP issued 45 findings of administrative violation, and imposed 27 penalty decrees.
Penalties	In 2011 CPDP imposed fines in the amount of BGN 75 100.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

1. With regard to the issued compulsory instructions and penalty decrees:

In 2011 compulsory instructions were issued in the following sectors: financial, state administration, communal services, transport, media, trade and services and telecommunications. Most often the instructions concerned:

- The necessary organisational and technical measures for guaranteeing that the level of protection of personal data was not decreased – 36%;

- Processing of personal data for purposes other than the declared purposes without notifying the CPDP about the change – 21%;

- Prohibition of processing specific categories of personal data – 18%;

- Not defining the retention period for storage of personal data – 16%;

- Violation of the provisions relating to informing individuals – 9%.

Among the most frequent breaches of the LPPD for which statements of administrative breaches were issued were:

- Breaches of personal data controller registration – for updating the information before making the change in the submitted data; – processing of data before entering the registers in the CPDP's system;

- Violation of the provisions on personal data protection measures – the necessary technical and organisation personal data protection measures were not implemented by the data controller (Article 23, paragraph 4 in connection with paragraph 1 of the LPPD);

- Violation of the principles for lawful personal data processing – data to be processed lawfully and in a bona fide manner, to be proportionate with regard to and not exceeding the processing purposes (Article 2, paragraph 2, p. 1 and p. 3 of the LPPD).

2. With regard to issuing opinions, notifications and requests:

Apart from the cases mentioned in the table, which were submitted to the CPDP by State authorities, the following opinions are of substantial interest:

2.1. Right of access to video recordings from video surveillance devices (in hospital) including information about third parties and whether the video surveillance is personal data – the CPDP issued an opinion that the video recordings from surveillance devices contain personal data, because they include information which can disclose the physical identity of the individual recorded, and in this regard every individual has the right to access to their personal data (including that recorded via video surveillance cameras). The personal data of specific individuals recorded by video surveillance cameras can be provided if it is technically possible to temporarily delete third parties' personal data, which could be disclosed by the exercise of this access right. In the event that third-party data cannot technically be temporarily deleted, the only legal grounds for exercising the access right would be the explicit consent of all other individuals – subject to the particular video surveillance.

2.2. The necessity to register data controllers which are neither established on the territory of the Republic of Bulgaria, nor in the territory of any European Union Member State:

– request for an opinion on whether Google/Google Inc. may record, on the territory of the Republic of Bulgaria, objects for their Google Street View service. The CPDP issued an opinion that, with regard to the processing of personal data for the purposes of the Google Street View service, the controller Google/Google Inc. has to appoint a legal representative in Bulgaria. In the opinion, the CPDP also gave compulsory instructions which have to be considered before, during and after the recording process: during the recording of street views cameras are not allowed to collect Wi-Fi data (data about wireless points of access); measures must be taken preventing the recording of payload data and other data

directly linked with individuals (email addresses, passwords etc.); the public must be informed about the rights of individuals in connection with the processing of their personal data for Google Street View purposes; and more restrictive measures must be taken such as technology to blur the images of individuals in places which are connected or could be connected with the processing of special categories of data etc.

3. With regard to the data transfer requests, other interesting cases include:

3.1. Request for authorisation of the transfer of – scanned biometric data to a company and another non-commercial legal entity in USA in connection with computer exams conducted in Bulgaria for the purposes of the admission of students to business schools worldwide. One of the main requirements for scanning the palm-prints of the candidates for the purpose of prevention of changing and/or substitution of candidates, and maintaining trust in the business schools to which admission was granted in the event of passing the test. The CPDP issued an opinion allowing the data controller/local representative to transfer scanned palm images (biometric data of individuals) – to the USA. The legal grounds for authorising the data transfer in this case was the existence of the explicit consent of the – test candidates, whose biometric data were the subject of the transfer.

3.2. Request for authorisation of the transfer of images and video recordings of the controller's employees and visitors to the workplace to the mother company in the USA. During the administrative procedure, the CPDP found the following shortcomings: there were no conditions for the admissibility of the processing; the necessity of the transfer with regard to visitors was not established; the data were excessive; and the processing was incompatible with the specific purpose of the request – human resources management. The CPDP refused to grant its approval to this transfer of data.

C. Other important information

1. With regard to the CPDP's activities related to the implementation of Directive 2006/24/EC in the Bulgarian legislation

Directive 2006/24/EC (Data Retention Directive) was transposed in the Bulgarian legislation in 2010 with the amendments and supplements in the Law on Electronic Communications (LEC). Upon these amendments entering into force all parties in the process of traffic data retention and access were legally determined, and the CPDP was appointed as the monitoring authority for data security. Pursuant to its competences under the LEC, in 2011 the CPDP for the first time summarised and provided statistical information in accordance with the requirements of the Law, the European Commission and the National Assembly within the deadline set by the LEC.

In this regard, 4 separate meetings of CPDP with interested parties as follows: competent authorities under LEC; undertakings providing electronic communication networks and/or services, prosecution and courts, were organised during September-December 2011.

The CPDP proposed for discussion and clarification issues such as – the usefulness of data obtained for the detection and prosecution of crimes by carrying out searches of people, as well as information regarding acquittals and guilty verdicts; the scope for submitting for analysis and summarising information about specific prevalent types of crimes or offences,, for which mostly access to traffic data is required; the scope for summarising information about the legal grounds and purposes for which the access is usually required; the observance of the obligation to keep registers for access requests, refusals, court authorisations and issued enquiries;- the scope for enquiry about cases of lengthy (6 months) data

retention periods in accordance with Article 250(a), paragraph 5 of the LPPD; cases where undertakings refuse to submit data; the data retention period (data age); clarification of the reporting period for undertakings submitting statistical information to the CPDP; the clarification of the scope for undertakings to submit more detailed information to the CPDP; clarification of the procedures for access to traffic data under the Penal Procedure Code for the purposes of pre-judicial and court proceedings

2. With regard to the CPDP's activity related to the training of data controllers on the implementation of the provisions of the Law for Protection of Personal Data and on specific questions

In 2011, the CPDP adopted a concept and a plan for training, and organised an extensive training campaign. For the preparation and the organisation of the training campaign current national goals and priorities were taken into account, which led to a series of training sessions aimed at improving the professional preparedness of personal data controllers and processors having access to the Schengen Information System, in view of the expected accession of the Republic of Bulgaria to the Schengen area. Simultaneously with the organisation of training on SIS, and following the practice of 2010, seminars were held with representatives of the local self-government authorities and the administration of the National Assembly of the Republic of Bulgaria. The CPDP also took part in the training courses of the Diplomatic Institute and the University of Library and Information Technologies.

In 2011, CPDP's training sessions were attended by data controllers from the public sector, private business, and the academic community. 22 seminars were held, including 12 for officials from institutions with access to NSIS; 3 seminars with local authorities and the National Association of the Municipalities in the Republic of Bulgaria; 2 training sessions of National Assembly staff; 1 for the Diplomatic Institute; 1 for the academic community; 2 for representatives of trade companies (NPP Kozloduy and EVN), and 1 for representatives from the professional branches (Bulgarian Pharmaceutical Union). In total 106 institutions have sent their representatives to participate in the training sessions, including 47 public institutions, 55 courts, 2 private companies and one branch organisation. The total number of trained people is 481 controllers and personal data processors, of which 333 took part in the training of controllers and processors with access to NSIS.

CYPRUS

A. Summary of activities and news

In September 2011 Mr Yiannos Danielides was appointed Commissioner for Personal Data Protection. Mr Danielides succeeded Ms Panayiota Polychronidou, who resigned from Office in June.

In our Office's efforts to promote awareness, in the frame of the activities organised for the European Day for Personal Data Protection, our Office used a budget of EUR 4 878 to distribute, on 28 January, to shopping centre visitor information flyers, measure tapes and CD protection pouches. The message of the day was "measures for protection".

A working document (draft bill) for the transposition of the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters was prepared by our Office in cooperation with the Cyprus Police.

In December 2010 a recognised refugee filed a complaint against a journalistic website which published copies of his ID card and other social welfare documents revealing the names, addresses and the monthly sum of public benefits that he and other asylum seeker refugees receive from the Social Welfare Services. After the examination of the complaint examination the Commissioner, taking into account the views posed by the website's lawyers and damage suffered by the complainant, issued a Decision concluding that the ongoing publication of the aforementioned data was in breach of the Law and imposed two administrative sanctions on the website, a fine of EUR 3 000 and the destruction of the data and the cessation of processing. As the website did not comply with the Decision, in April the Commissioner, in accordance of the power vested in her by Section 23(a) of the Law reported the case to the Chief of the Police to examine the possibility an offence committed by the website, in accordance with Section 26 of the Law.

Our Office examined a complaint against the Cyprus Telecommunications Authority (CYTA) from an employee who was refused the right to access information relating to a disciplinary procedure against him initiated after an accusation and, in particular, the name of the accuser. The CYTA concluded that the accusation was not founded, did not conducted a disciplinary inquiry and provided the complainant with all the relevant documents but it refused to disclose the accuser's identity as requested by the complainant for the purposes of taking legal action against him. The Commissioner issued a Decision concluding that all data included in an accusation letter constitute personal data relating to the data subject and that; in this case, the request for access was partly satisfied. The CYTA was called to provide the complainant with a copy of the accuser's letter and to disclose his identity.

In view of the coming Commission Proposal(s) for the reform of the European Data Protection legislation our Office accepted the Ministry of Justice and Public Order request to represent the Republic at DAPIX, the Council's Working Party which was expected to discuss the Proposal(s) under the Polish Presidency. A number of Officers undertook specialised training at the Academy of Public Administration designed to assist them with their new Council and upcoming Cyprus Presidency responsibilities, and discussions with the Ministry and the Police were initiated for formulating a procedure for the adoption of common positions.

Organisation	Office of the Commissioner for Personal Data Protection
Chair and/or College	Mr Yiannos Danielides
Budget	Allocated budget EUR 297033 and executed budget EUR 28 472
Staff	Administrative Officers: 7 Information Technology Officers: 2 Secretarial Officers: 6 Auxiliary staff: 2
General Activity	
Decisions, opinions, recommendations	Number of Opinions: 11 Number of Decisions: 7 Number of Recommendations: 4
Notifications	Number of notifications: 162
Prior checks	Number of prior checks: N/A
Requests from data subjects	Number of requests received in writing or by phone by data subjects: N/A
Complaints from data subjects	Number of qualified complaints: 469
Advice requested by parliament or government	On 8 occasions our Office was invited by the House of Representatives of Cyprus to make consultations and participate in meetings before the competent Parliamentary Committees.
Other relevant general activity information	Number of licences for the combination of filing systems: 18 Number of transmission to third countries licences: 48
Inspection activities	
Inspections, investigations	Number of inspections and/or investigations: 22 In 2009 inspections on the banking sector were carried out. In 2010 our Office issued relevant Guidelines and initiated a follow-up inspection to monitor banks' compliance, which was concluded in 2011. The Report of the outcomes of the follow up showed that 16 out of 18 commercial banks operating in Cyprus were in compliance with the Guidelines. The other 4 inspections carried out in the framework of the

	examination of complaints with regard to the installation of CCTV systems.
Sanction activities	
Sanctions	Number of sanctions decided by the DPA: 7 Number of legal actions started by the DPA against data controllers for the collection of penalties: 2
Penalties	Amounts imposed by DPA: EUR 13 000
DPOs	
Figures on DPOs	N/A.

CZECH REPUBLIC

A. Summary of activities and news

The supervisory activity was partly based on the DPA´s inspection plan, partly initiated by data subjects´ complaints. An account of the typical or most interesting cases is provided below. Generally, the inspection plan intended to focus on government information systems (such databases have proliferated over recent years), information systems operated by private entities (e.g. customers´ cards, loyalty cards), and data processing operations for the purpose of crime prevention and fight against terrorism. Complaints lodged by citizens concerned mostly video surveillance, posting of personal information online, and data processing conducted by financial institutions or electronic services providers.

In the summer, the Office successfully completed an international project (jointly with the Hungarian and Polish DPAs) "Raising awareness of data protection issues among the entrepreneurs operating in the EU", funded from the Leonardo da Vinci Partnership program under the number CZ/09/LLP-PS/P/LdV/061. The project was devoted to workplace privacy and protection of employee data from the employer´s perspective. The main output was a comprehensive handbook and a series of dissemination activities.

Two staff members worked on several occasions as short-term experts in Skopje/FYROM within the technical assistance project "Support to the Directorate for Personal Data Protection" (EuropeAid/128570/S/CER/FYR).

Organisation	Office for Personal Data Protection
Chair and/or College	Mr Igor Němec (President of the Office)
Budget	CZK 262 175 040 (EUR 10 487 001, exchange ratio 1 EUR = 25 CZK) – out of which EUR 3 073 800 was received from EU structural funds, especially for a project concerning creation of a government central register.
Staff	99
General Activity	
Decisions, opinions, recommendations	3 opinions (all related to processing operations in the private sector).
Notifications	4421 notifications (out of which 3856 registered, 1002 still ongoing or suspended).
Prior checks	82
Requests from data subjects	2294 (out of which 110 from abroad).
Complaints from data subjects	1119 (plus another 4613 concerning spam).
Advice requested by parliament	No such request in 2011.

or government	
Other relevant general activity information	23 requests pursuant to Free Access to Information Act. 75 bills and 91 implementing regulations commented within inter-ministerial comments procedure. International transfers authorization: 9 requests of which 3 permitted, 6 suspended due to procedural reasons.
Inspection Activities	
Inspections, investigations	179 (out of which 144 accomplished) + 157 investigations concerning spam (out of which 137 accomplished).
Sanction Activities	
Sanctions	ca. 70 sanctions. Explanatory note: Under sanction we understand a non-financial remedial measure imposed on a controller. Within one investigation we often imposed a number of different sanctions (remedial measures), however for the purposes of this information, a set of sanctions under a particular investigation is counted as one. Average on one action is about 2,7.
Penalties	ca. 105 penalties.
DPOs	
Figures on DPOs	Not applicable in the Czech Republic.

B. Information on case-law

In 2011, the Czech Republic organized a **census** (within the worldwide action). One of the Office´s inspectors conducted an inspection at the Czech Statistical Office. It acted upon a number of complaints filed by citizens who had complained about the method of the census, as well as about the retention of anonymized forms at the National Archive (and retention of the census results at the Czech Statistical Office). The inspection was started in mid-2011, and was not concluded by the end of the reference year.

The Office performed an **inspection of the online version of the Companies register,** which was part of the e-government system. Personal data are processed via this portal (operated by the Ministry of Justice), creating a higher risk of potential misuse, given the online environment. The inspector pointed out that for each data processing operation there must be a designated controller bearing responsibility for legal compliance. Moreover, the inspector stated, the scope of data (or documents) collected is prescribed by the Directive 2009/101/EC, and posting of other documents must be carefully considered against the purpose limitation principle. Similarly, the retention period of these online personal data must be in proportion to the purpose (availability of eligible information to third parties). Another issue revealed by the inspection was the disclosure of birth numbers (i.e. identification numbers assigned to each newborn child). Thanks to this inspection revealing this issue, the Office succeeded on including in the amended

version of the Commercial Code a provision that birth numbers should not be published either in the extract from the Companies register, or in the Commercial journal.

Many municipalities use video cameras to record or transmit their sessions in real time. The issue of **video records and transmissions** of municipal council meeting is closely observed both by the public and journalists. The Office therefore initiated several on-the-spot investigations, and issued some principles later: The municipal council must always clearly state the purpose of the audio or video record. If a meeting is covered in whole, without adaptations, then the document is governed by the law on archives. Such document may then serve only as source for the meeting minutes, and must be destroyed after the minutes are written. If the municipal council provides online streaming of a meeting (without making a record), no personal data processing is involved, and the Data Protection Act does not apply.

In respect of the rapidly emerging issue of electronic communications in the area of government information systems, the Office focused on the level of security guaranteed for **electronic operations performed by public authorities through data boxes** operated within the data box information system, in conformity with the Electronic Operations and Authorized Conversion Act. The Office commenced an inspection at the Ministry of Interior, which was the controller, and at the Czech Post, as the operator of this system. It was subsequently found necessary to extend this inspection to the Ministry of Justice. The number of complaints increased in 2010 and 2011 in respect of the delivery of court documents addressed to attorneys-at-law to the data boxes of natural persons operating a business. It followed from a statement of the Ministry of Justice that documents had been erroneously served by a number of courts; this followed from the results of investigation pursued by the supplier of information systems. In addition, the Ministry of Justice also records individual complaints. On the basis of this information, an inspection was initiated (also in conformity with the inspection plan priorities). The inspection was concerned particularly with the systemic conditions created for the performance of the administrators' duties in processing personal data within the so-called Data Box Information System, with special emphasis on the performance of duties in securing personal data. Bearing in mind that the main objective of an inspection is to provide for a remedy and create system conditions for eliminating human errors, three on-the-spot investigations focused on the staff of the Ministry of Interior responsible for the installation and administering of the data boxes. Employees of the Ministry of Justice were also invited to the closing investigation, particularly because all complaints lodged were concerned with courts. According to statements made by the representatives of both ministries, a separate flag should be introduced for attorneys-at-law as from the date when data boxes are compulsorily established for attorneys.

C. Other important information

In the margin of the Privacy and Data Protection Commissioner´s conference in Mexico City in October, one of the Czech delegates possessing the authority of investigation conducted an **inspection at the Czech embassy** in Mexico. The purpose of the inspection was to meet the commitments within the Schengen evaluation process. Later this year, similar inspections were conducted at the Czech embassies in Macedonia and Moldova.

The European Personal Data Protection Day in January has traditionally offered the opportunity to organize an **awareness raising** event. This year, the Office announced what is already the fifth edition of the successful competition for children and youth titled "This is my privacy! Don't look, don't poke about!" In preparing the event the Office co-operated again with Czech Radio Prague, the International Festival of Films for Children and Youth in the City of Zlín, and this time also with the Association of Library and Information Professionals. In more than 100 libraries throughout the Czech Republic, children from 7 to 10 years of age competed in the Through the Wild Web Woods game, which teaches them in an amusing way how to behave safely and respectfully on the Internet. In devising the Czech version of the game the

Office co-operated with the Council of Europe, which had prepared this entertaining form of training for safe behaviour in the Internet.

The Office´s experts took part as **lecturers** in about 40 local events held for academic, legal, business and public law entities on the topic of the protection of personal data.

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. Cases of a principle interest (approximately 15 cases per year) are put before the Council for decision. The Council is chaired by a Supreme Court Judge.
Budget	DKK 20.3 million
Staff	Approximately 35
General Activity	
Opinions, recommendations	N/A (included in figures below).
Notifications	2 602
Prior checks	2 602
Requests from citizens	1 965 (this number covers all requests and complaints made to the Danish DPA)
Complaints from citizens	See above.
Advice requested by parliament or government	339
Other relevant general activity information	51 cases relating to security
Inspection activities	
Inspections	54
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 2 cases.
DPOs	

Figures on DPOs	N/A (this is not an option according to Danish legislation).

B. Information on case-law

The use of fingerprint in registering participation in a mandatory course in order to receive social benefits

A Danish trade union wanted to make a complaint on behalf of a member. The local municipality had started a practice whereby unemployed people participating in a course were required to register their fingerprint in order to show their attendance.

The municipality explained that the purpose of processing this information was to register the attendance on the course which the municipality's unemployed people were required to attend in order to receive their social benefits.

The municipality further explained that only a numeric number (template) of the fingerprint was collected and processed in the system.

Finally the Municipality explained that it was necessary for them to use fingerprints in order to effectively administer attendance and safeguard against misuse, and that the municipality found the use of biometric information to be in accordance with the Danish act on processing personal information.

The Danish DPA found that the processing was necessary for the performance of a task carried out in the exercise of official authority because of the Municipality's obligations and the DPA did not oppose the Municipality's use of fingerprints in order to register the attendees without the consent of the data subject in accordance with Section 6, subsection 6 of the Danish Act on Processing of Personal Data.

Counselling of grieving children and young people

In 2011 the Danish DPA gave permission to a counselling centre who were providing counselling for children and young people in periods of grief.

The counselling centre's primary purpose was to comfort and counsel children and young people who had experiences with death or serious illness in their immediate family.

The counselling centre would process personal information about both the child and young person, but also about relatives of the child/young person. The information regarding the child receiving the counselling would be processed with consent as the legal basis. In regards to family members, both dead and alive, it would not be possible and feasible to require consent as the legal basis.

The Danish DPA decided that the processing of personal information regarding family members should be allowed and for the first time used Section 7, paragraph 7 of the Danish Act on Processing of Personal Data which builds on Article 8 paragraph 4 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Danish DPA felt that the purpose in this case met the substantial public-interest requirement in Article 8, Section 4 in the Directive.

C. Other important information

International data protection day

The Danish DPA spent international data protection day in a nearby shopping centre trying to educate and inform the general public about data protection. The staff answered questions, distributed flyers with relevant information among the visitors at the centre and facilitated an online quiz regarding data protection. The day was a great success for both staff and visitors who showed a great knowledge and interest in data protection.

Danish BCR

In 2011 the Danish DPA completed the first BCR as lead when the Danish company Novo Nordisk A/S received their BCR. The work on the Novo BCR started in 2007 and the Danish DPA has subsequently been contacted by other Danish firms who also want to have a BCR.

ESTONIA

A: Summary of the activity and news:

Organisation	
Chair and/or College	Estonian Data Protection Inspectorate
Budget	EUR 592 446
Staff	18 (supporting services like IT and accounting is out-sourced).
General Activity	
Decisions, opinions, recommendations	Decisions: 354 Supervisory decisions (including 114 refusals to initiate and 38 precepts); 58 Misdemeanour decisions; 9 Appeal decisions and 18 permission decisions (7 permissions for science research and 11 permissions for data transfer). Opinions (guidelines): **3** (Data protection in working life; Guidelines for human resources employees: Personal Data in Employment Relationship and Informing about children who need help and data protection). Recommendations: **130** for the better arranging of data protection.
Notifications	327 (processing sensitive data).
Prior checks	0
Requests from data subjects	**687** by email/mail (195 public sector; 257 private sector; 110 non-profit sector; 37 media, 53 social-networking; 35 spam and **615** helpline calls.
Complaints from data subjects	**413**
Advice requested by parliament or government	**2** (regarding the Population Register Law; Electronic Communications Law).
Other relevant general activity information	**41** opinions on draft acts by request on government.
Inspection activities	
Inspections, investigations	Inspections: **77** on-site. Investigations: **7** (Compliance and adequacy audits) Comparative monitoring: **3** (among employers; security measures in municipalities; direct marketing).

Sanction activities	
Sanctions	**38** Coercive payments and fines for misdemeanours.
Penalties	3824 88 (by DPA).
DPOs	
Figures on DPOs	**126** new notifications of DPOs + **9** changes of DPOs.

B. Information on case-law

Estonian-Latvian Cooperation – Joint supervision of Stockmann

Estonian and Latvian DPAs performed joint supervision of Stockmann department stores in Estonia and Latvia regarding personal data protection in labour relations and customer relations, including direct marketing.

Supervisors suggested that Stockmann Group affiliates make clearer notification for clients regarding data collecting, the terms of direct marketing and the closure and deletion of customer data at their request. Also the DPAs suggested that Stockmann distinguishes the mandatory fields of data that have to be given in order to become a Stockmann Loyal Customer. The authorities asked Stockmann to add a section containing information about the possibilities of deletion of personal data from the database.

In addition, the supervisors pointed out that if the customer gives permission for receiving commercial information, Stockmann only has the right to ask for a relevant contact address (postal, email, mobile phone etc.) for delivering messages. Another issue that needed to be addressed is regarding the profiling of clients – the clients have to be informed about it in order to make a decision to become a loyal customer of Stockmann.

C. Other important information

We carried out an extensive **internal audit of administrative procedures with an analysis of court judgements and legal literature.** The goal was to harmonise the legal practice of the Inspectorate, to guarantee that it is understandable and justified, and to reduce procedural errors. We framed our detailed manual of administrative procedures.

The other major topic analysed was the **contact between private life and freedom of expression**. Not many cases like this are taken to court and they mainly focus on the issue of libel. Restricting freedom of expression must be a well-considered decision. We carried out a thorough analysis of the rulings made by the European Court of Human Rights, the existing literature (of which there is a shortage in Estonia) and the rulings made by the Supreme Court. This is the basis we can rely on when resolving complaints and justifying our decisions. We also arranged a joint seminar with the Estonian Newspaper Association, which was held in April this year.

Information exchanges with the Police and Border Guard Board and the Ministry of the Interior for surveillance of the misuse of police databases and the Population Register, respectively, are on firm

grounds. Misuse of the Population Register was increasing, so we discussed the problem in the media and implemented a stricter fine policy.

We also started a **regular information exchange with the Estonian eHealth Foundation** in order to monitor the misuse of patient data.

FINLAND

A. Summary of activity and news

The emphasis of the work was on preventative operations. Increased impact was sought through accurate targeting of general guidance and functional integration with various groups, committees and other similar organisations. A representative from the Office of the Data Protection Ombudsman participated in the work of an approximate total of 80 advisory committees, working groups or similar cooperative organs. The Data Protection Ombudsman has been a member or expert member in the information security group of the Information Society in Everyday Life programme, ended on 28 February 2011, as well as in the Government Information Security Management Board VAHTI. He is also a member of a monitoring group on the codification of the information society established by the Ministry of Transport and Communications on 9 December 2011. The term of office for the monitoring group will continue until 31 October 2014. On 14 October 2011, the Ministry of Justice invited the Data Protection Ombudsman to participate in the work of a panel supporting the preparation of a national human rights action programme. The term of office for the panel was from 14 October 2011 to 31 January 2012.

Representatives of the Office have participated in several working groups under the Government Information Security Management Board VAHTI as well as the approximately 30 working and steering groups established by various administrative branches. Cooperation has also been continued to establish codes of conduct or other branch-specific guidance, among other things.

At the end of the 24th year of operations for the Office of the Data Protection Ombudsman, an unprecedented wave of data protection breaches occurred in Finland. News and revelations of leaked personal information were published almost on a weekly basis. Still, according to the information gathered by the CERT unit of our partner, the Finnish Communications Regulatory Authority, the publically discussed cases were only a small part of all the data leaks occurring in the same period. The fact that Finnish regulations do not include an actual obligation to report the leaks to the persons whose information has been leaked was considered a problem of particular interest. The trust that citizens placed in the services of the information society was severely tested.

Safer Internet Week focused on social media and privacy on the Internet

The Office of the Data Protection Ombudsman participated once again in the activities of the Safer Internet Day and Week on 8 February 2011. The Safer Internet Day, now organised for the eighth time, is part of the national information security strategy. This year, the campaign focused on privacy on the Internet. Information security for social media was also discussed from a broader perspective.

Social media has brought the problems of online information security closer to the ordinary user. The safe use of online communities requires care and attention, and privacy protection is increasing in importance. Before the Safer Internet Day, the Information Security Guide website was updated with new information on fraudulent links, privacy protection and the safe use of the social media.

Schoolchildren and teens are often more experienced users of online communities than adults are, but still need at least as much guidance for safe surfing and protecting their privacy. Various exercises on the subject were published for schools, as well as a contest on the Online Safety School website (www.tietoturvakoulu.fi).

The Safer Internet Day also gained better visibility on the Internet. The Suomi24 discussion forum carried a specialist section on the Safer Internet Day for the whole of February. In the section, specialists involved in the Safer Internet Day campaign answered the users' information security- related questions.

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 1 585 000
Staff	The total number of staff is 20
General Activity	
Decisions, opinions, recommendations	2 630
Notifications	377
Prior checks	See notifications
Request from data subjects	950
Complaints from data subjects	(access and rectifications) 189
Advice requested by parliament or government	93
Other relevant general activity information	Cooperation work with data controllers in the following sectors: Education, Health Care, Social Affairs, Telecommunications, Employment and Economy.
Inspections activities	
Inspections, investigations	654
Sanctions activities	75
Sanctions	N/A

Penalties	N/A
DPOs	
Figures on DPOs	>1000

B. Information on case-law

– An applicant, in the exercise of his right of access, had requested the controller to provide to him recordings of any of his customer calls to the corporation.

The right of access of the applicant as defined in Section 26 of the Personal Data Act applies to existing customer call recordings, unless a basis for a restriction on the right of access in accordance with Section 27 of the Personal Data Act exists. In its explanation, the controller did not assert any such basis for restricting the applicant's right of access for the recordings in question. Thus, the controller had the obligation to provide the information in question to the applicant, as specified in Section 28.2 of the Personal Data Act. The controller was obliged either to give the applicant an opportunity to listen to the call recordings, or to provide a written account of the content of the recordings upon the request of the applicant.

– A person requested the Data Protection Ombudsman to take measures due to a message he had sent to the city construction office having also been sent to the city planning department, and having thus been made public. The message concerned matters related to street maintenance and parking in the street.

The level of publicity of a document that is delivered to an official is defined based on the Act on the Openness of Government Activities (621/1999). Each public official makes independent decisions on the confidentiality of documents and other duties according to the Act on the Openness of Government Activities. The Data Protection Ombudsman has no general obligation to guide or supervise compliance with the Act on the Openness of Government Activities, nor the right to interfere in the decisions based on it by other officials.

– The National Institute for Health and Welfare had reserved the Data Protection Ombudsman for an opportunity to be heard in the manner stipulated by Section 4, Subsection 1 of the Act on National Health Care Customer Registers (556/1989, revised in 38/1993). A statement was requested on the application of a group of researchers to receive information for their study from the Care Registers for Social Welfare and Health Care HILMO, maintained by the National Institute for Health and Welfare.

As the received additional explanation showed that it was not the intention to connect the information or samples collected from research subjects with their permission to the register data being requested, it seemed that there was no obstacle for transferring the information after the appropriateness of some unclarities mentioned in the application was confirmed and other research data was obtained in a legal manner.

– The Data Protection Ombudsman received a question on whether camera surveillance used in the outdoor areas and in the shared indoor facilities of a professional foster home was legal. The professional foster home was also the home of the people working in it 24 hours a day. There was no sign indicating the presence of camera surveillance. A description of the file existed, but it was not available at the home. Consent for surveillance in the indoor facilities had also not been requested.

The primary question was whether camera surveillance in the shared living area of the foster home was in general allowed based on legal stipulations on fundamental rights, criminal law, the Child Welfare Act or other particular legislation. Foster home operations are organised in accordance with the Child Welfare Act, which means that the Ministry of Social Affairs and Health has the jurisdiction to comment on what kind of situations would provide the necessary justification for camera surveillance of the operations in question. It is the view of the Data Protection Ombudsman that the question of whether it was permissible according to the Personal Data Act (523/1999) or the Act on the Protection of Privacy in Working Life to handle the personal data of the inhabitants and staff through camera surveillance was only of secondary importance in the matter.

C. Other important information

The first PIA (Privacy Impact Assessment) evaluated

A major Finnish retail corporation that maintains a regular customer database made changes to its bonus card system. At the same time, it adopted RFID technology for its cards. Due to this change, the corporation performed the PIA and submitted it to the Data Protection Ombudsman for assessment.

In Finland, there was also a working group that assessed the potential need for legislation on Near Field Communication technology. The working group adopted the stand that the coverage of the general data protection legislation is adequate also for NFC technology.

Actions to improve national information management

The Finnish Government issued a decision in principle on the availability of public data materials. The aim is to improve the opportunities for more extensive utilisation of our national data deposits (open data), while maintaining respect for personal data protection. The presentation was also supported by the new Data Administration Act that aims at the adoption of a national information architecture consisting of compatible elements.

The implementation of a data protection decree based on the Act on the Openness of Government Activities, which regulates the proper data administration for official information materials and personal data files, also proceeded during the year under review. The purpose is to ensure that all units in state administration achieve a certain level of information security corresponding to their operations.

Data protection in various fields

The Office of the Data Protection Ombudsman has organised supervised stakeholder cooperation in the fields of education, data communications, health and social care, marketing and scientific research, among other areas. These working groups have discussed issues related to themes such as youth well-being services, information systems used for educational purposes, mobile certification and the utilisation of basic Finnish data registers in research.

Branch-specific surveys were carried out to examine the level of data protection in various sectors. The surveys also provided an opportunity to distribute information and guidance on the subject to controllers.

FRANCE

A. Summary of activity and news

Amendment of Directive 95/46: successful data protection in Europe

A strategic priority for the European Commission and for the CNIL (French Data Protection Authority), which met with the departments of the European Commission responsible for drafting the new instrument. Based on its 30 years of experience, the CNIL supports a participatory and decentralised data protection system that it feels is most suited to the digital world and the diversity of the situations encountered in the field, involving several areas of the law, whether relating to employment, criminal, tax or corporate law, etc. that only the national authorities are in a position to know. European governance of data protection, in order to be effective and democratic, must be based on close cooperation between competent sovereign authorities.
The CNIL found it useful to meet several MEPs in May 2011 within the context of the European Commission's draft parliamentary report on communication. Lastly, the Chairman of the CNIL met Mrs. Reding in Paris on 26 November 2011. This meeting was an opportunity for the CNIL to reaffirm its position with regard to the direction taken for the draft regulation.

Monitoring of technological developments

The cloud

In October 2011, the CNIL launched a consultation on the subject of "*Cloud computing*" with professionals, in order to anticipate all of the legal and technical solutions that would guarantee a high level of data protection, while taking into account the associated economic challenges. The questions covered five topics: definition of the cloud, qualification of the cloud provider, determination of applicable law, management of transfers and cloud security. At the end of this consultation, all of the contributions were published on the CNIL website (www.cnil.fr) and could be used within the context of G29 work on this subject.

Labels

The first two public evaluation reference bases enabling the CNIL to label audit procedures for the processing of data and "Data Protection" training were published on 3 November 2011.
Any body whose audit procedure for processing or training corresponds to the content defined by the reference bases adopted by the CNIL can now submit a label request. It just needs to complete the form provided for this purpose and provide all of the information requested.
The label is therefore a double guarantee of quality and compliance with the requirements laid down by the law and by the CNIL. The approach is presented on a dedicated "CNIL Labels" page of the CNIL website (www.cnil.fr). A page specific to each label completes the description of the device.

Google

Lastly, the CNIL has sanctioned Google for the mass collection of technical Wi-Fi data without the data subjects' knowledge, and the capture of so-called "content" data (logins, passwords, connection data, email exchanges). The CNIL served GOOGLE with formal notice in May 2010 to resolve the situation. Given that it had not responded to its requests within the allotted time, the administrative claims section of the CNIL issued the company with a €100,000 fine on 17 March 2011.

Inspection and awareness-raising actions

Inspection of all video surveillance systems

The LOPPSI law of 14 March 2011 on internal security gave the CNIL the authority to inspect all video surveillance systems installed on public roads or in public places. Previously, the CNIL only had authority to inspect systems installed in places that are not freely accessible. This long-awaited change now enables implementation of a consistent and independent inspection of all video surveillance systems installed in France.

Practical guides

Furthermore, the CNIL continued its work to raise awareness in 2011, in particular publishing two practical guides (for lawyers and for healthcare professionals), as well as a recommendation on policy communication.

Organisation	
Chair and/or College	Chair: Isabelle FALQUE-PIERROTIN, Vice-Chairman: Emmanuel de GIVRY, Jean-Paul AMOUDRY 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 2011 (in million EUR 15.8
Staff	Number of staff: 159
General Activity	
Decisions, opinions, recommendations	1 969 decisions (+ 25.5% more than in 2010) / 93 opinions / 1 recommendation.
Notifications	82 243 notifications to the CNIL, including: 5 993 notifications for video-surveillance systems (+37% more than in 2010). 4 483 notifications for geolocation systems (+ 33.5% more than in 2010).
Prior checks	Authorisations: 1 759 in 2011, including: 249 authorisations adopted in the Plenary, 887 data transfer authorisations to non-EU States, 6 framework authorisations, 744 authorisations for biometric systems (+ 5.4% more than in 2010), 503 authorisations for processing of personal data for the purpose of medical research, and 120 authorisations for processing of personal data for the

	purposes of evaluation or analysis of care and prevention practices or activities.
Requests from data subjects	Requests from the public: In 2011, the CNIL received 32 743 writings (+10% more than in 2010) and 138 979 calls (+4.6% more than in 2010).
Complaints from data subjects	The CNIL received 5 738 complaints in 2011 (+ 19% more than in 2010). This is the highest number of complaints ever received by the CNIL. The main issues of complaints were related to the right to be forgotten and to video-surveillance systems. Requests from data subjects: 2 099 requests for indirect access where processing involves State security, defence or public safety (+ 12% more than in 2010).
Advice requested by parliament or government	In 2011, the CNIL adopted 92 opinions on national draft regulations (i.e. 20% of the total 425 opinions adopted by the Plenary). Furthermore, the CNIL was auditioned 23 times by the Members of the French Parliament, and had 10 meetings with Members of the French Parliament for an exchange of views about data protection issues.
Other relevant general activity information	-
Inspection activities	
Inspections, investigations	385 investigations (+25% more than in 2010), including 151 investigations related to video-surveillance systems.
Sanction activities	
Sanctions	18 Sanctions taken by the CNIL in 2011. Legal actions against data controllers: 83 (65 formal notices to comply, 5 financial penalties, 13 warnings), 2 discharges.
Penalties	Total amount EUR 190 000, imposed by the CNIL in 2011.
DPOs	
Figures on DPOs	8 635 bodies appointed a DPO (+25% more than in 2010).

B. Information on case-law

Below is a list of the main decisions returned by French jurisdictions in relation to personal data protection:

- Caen Court of Appeal, 3rd chamber, social section 1, Workplace Health and Safety Committee (CHSCT) of the company Benoît GIRARD v Trade Union (CFDT) of metallurgy industry employees in the Caen region, 0903336 (23 September 2011)

- Montpellier Court of Appeal, chamber 5, section A, Marie-Cécile C v Google Inc, 1100832 (29 September 2011)
- Paris Court of Appeal, Division 5, chamber 11, SAS ANTIK BATIK v SA SAFETIC, 0920824 (9 September 2011)
- Supreme Court of Appeal, 1st civil chamber, company NORD-OUEST et al v company DAILYMOTION, 0967896165 (17 February 2011)
- Supreme Court of Appeal, commercial chamber, Ceramconcept v Administration des Impôts (Tax Authority), 1015014 (27 April 2011)
- Supreme Court of Appeal, criminal chamber, Movsar X and Zarea Y, 1084344 (11 May 2011)
- Supreme Court of Appeal, criminal chamber, Schering-Plough v DGCCRF (Directorate General for Competition Policy, Consumer Affairs and Fraud Control) 1085479 (29 June 2011)
- Supreme Court of Appeal, social chamber, M D v company MOREAU Incendie, 1018036 (3 November 2011)
- Supreme Court of Appeal, social chamber, M. X. v Méditerranéenne de Nettoiement, Groupe Nicollin, 1014869 (21 September 2011)
- Supreme Court of Appeal, social chamber, Mrs T v company UFIFRANCE Gestion, 1014685 (5 July 2011)
- EC, Association pour la Promotion de l'Image et al, 317827 (26 October 2011)
- Administrative Court of Clermont-Ferrand, SA Notrefamille.com, 1001584 (13 July 2011)
- Administrative Court of Strasbourg, O A, C M, A Z v Prefect of Bas-Rhin, 0902015 (5 October 2011)
- Administrative Court of Strasbourg, O A, C M, A Z v Prefect of Bas-Rhin, 0902016 (5 October 2011)
- Commercial Court of Nanterre, Greenpeace v Thierry L EDF, (10 November 2011)
- Court of First Instance of Charleville-Mézières, Philippe D et al v Jean-Luc P et al, 10349000004 (24 February 2011)
- Court of First Instance of Coutances, René L v Stanislas L, 1000822 (6 October 2011)

GERMANY

A: Summary of activities and news:

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 additionally in Bavaria a separate supervisory authority for the private sector.

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

Organisation	Federal Commissioner for Data Protection and Freedom of Information
Chair and/or College	Peter Schaar
Budget	EUR 8 765 000
Staff	85 in total Head office: 4 Division I: 4 Division II: 13 Division III: 8 Division IV: 7 Division V: 6 Division VI: 9 Division VII: 7 Division VIII: 9 Division IX: 4 Central Services: 12 Press office: 2
General Activity	
Decisions, opinions,	N/A

recommendations	
Notifications	N/A
Prior checks	N/A
Requests from data subjects	9 143
Complaints from data subjects	5 161
Advice requested by parliament or government	N/A
Other relevant general activity information	N/A
Inspection activities	
Inspections, investigations	N/A
Sanction activities	
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	N/A

1. Data protection in the employment sector

In Germany, the German Bundestag is still debating the draft Act Governing Data Protection in the Employment Sector (complementing the Federal Data Protection Act). However, given Article 82 of the EU's Draft Proposal for a General Data Protection Regulation, it is questionable whether the bill will be adopted.

2. Implementation of Directive 2005/60/EC – Act on Improving the Prevention of Money Laundering

The Act on Improving the Prevention of Money Laundering of 22 December 2011 (Federal Law Gazette I 2011, 2959) thoroughly revised the Money Laundering Act (GwG). Most importantly, due diligence, reporting requirements and internal security measures have been intensified and extended, and the circle of those who need to fulfil these obligations has been expanded. The new act has lowered the threshold for intervention in the case of violations of due diligence obligations.

Extending due diligence obligations also means that the enterprises, institutions or persons under this obligation according to the GwG have to fulfil more comprehensive data storage or data-gathering requirements, which also increases the administrative burden. The considerable fines imposed in the case

of violations of due diligence are also likely to increase the pressure so that those having to fulfil these obligations are even more inclined to gather data from contractual partners and, if necessary, forward them to the Federal Criminal Police Office and law enforcement authorities to avoid such fines. This also undermines the principles of data avoidance and data economy, since the combination of extended due diligence obligations and more severe sanctions lead to the collection of even more data. Increasing the number of economic sectors required to fulfil these obligations can also bear the risk of comprehensive data collection in financial transactions. Furthermore, the threshold for suspicious transaction reports has been considerably lowered. In general, introducing stricter due diligence obligations and lowering the threshold for suspicious transactions constitute a serious interference in an individual's right to determine the use of his or her data pursuant to Article 2(1) in conjunction with Article 1(1) of the Basic Law (GG), since financial transactions are increasingly subject to forced and comprehensive transparency. Hence, there is a risk that the far-reaching collection of personal data intended by the act – irrespective of levels of suspicion – will lead to the excessive monitoring of financial transactions, since the enterprises, institutions or persons under this obligation are even more inclined to gather data proactively and forward them to law enforcement authorities.

B. Information on case-law

1. In its ruling of 12 October 2011, 2 BvR 236/08, the Federal Constitutional Court decided on the revision of covert investigation measures in criminal procedures, including the differentiation concerning the protection of communication with persons bound by professional secrecy. Communication with the press and medical doctors, for example, is generally less protected than communication with members of the clergy. The rules on the protection of the inviolable core of an individual's private sphere in the interception of telecommunications were also approved by the Court. The amendment had been met with major criticism.

2. In its ruling of 24 January 2012 the Federal Constitutional Court pointed out that a request for information on telecommunications data always requires an authorisation for data transmission and a legal basis for the request. For this reason the storage and transmission of telecommunications data to investigative authorities were declared unconstitutional, because these authorities have access to passwords and PIN codes. Thus the investigative authorities are able to read and search data stored on a confiscated mobile phone while it was not necessarily clear whether the authorities are authorised to do this.

Furthermore the Federal Constitutional Court clarified that a request for information on the subscriber of a dynamic IP address constitutes a violation of the privacy of telecommunications. In order to identify a dynamic IP address, telecommunication companies must search the call data of their customers and access specific telecommunication procedures which are subject to Article 10 of the Basic Law. German law-makers must create clear provisions for this matter ensuring the protection of extremely sensitive call data.

C. Other important information

Draft Act to Promote Electronic Government (E-Government Act)

Currently, a draft act to promote electronic government, the E-Government Act, is being debated. The act aims at removing legal obstacles to facilitate electronic communication particularly between citizens and public administration. Essentially, this will be achieved by adopting technically secure procedures to

replace documents in writing, e.g. by including the new ID card's online function and by providing secure and trusted communication possibilities on the Internet. The draft act also includes the following points:

- Requiring public administration to provide electronic access;
- Allowing citizens to provide electronic proof in administrative procedures;
- Introducing electronic files in federal authorities;
- Providing machine-readable data by the administration ("open government data").

The debate on the draft act will also focus on ensuring that the removal of obstacles to fully implement electronic administrative processes without media inconsistencies will not lead to a reduction of the data-protection level guaranteed by the public administration. For this reason one priority is to design and organise technical processes in line with data-protection standards.

GREECE

A: Summary of activities and news

Recently the Hellenic Parliament passed Law 4055/2012, which comprises certain provisions regulating matters pertaining to the operation of the constitutionally safeguarded independent authorities in general, and in particular, the Data Protection Authority. The above law provides for a prior proposal by the Parliamentary Committee on Institutions and Transparency to the Conference of Presidents of the Parliament for the selection of the authorities' presidents and members for a non-renewable six-year term of office. Furthermore, it stipulates that the status of exclusive, full-time employment is also extended to the vice- or deputy-president of each independent authority, with the possibility of further extending this status of employment to a number of board members of each authority. It also provides for the employment status of the scientific staff members, who carry out the main mission of each authority, to be the same for all independent authorities. Moreover, Law 3917/2011: a) incorporated into our national law Directive 2006/24/EC, b) included provisions regarding the use of video surveillance systems in public areas and c) amended certain provisions of Data Protection Law 2472/1997, the most important of which gave the power to the DPA to prioritise the complaints and requests to be handled according to the importance and the general interest of the issue. The rest of the amendments concerned matters relating to the DPA's composition and secondment of public employees to the DPA. Finally, amendments were included to certain provisions of Law 3471/2006 relating to the lawful receipt of unsolicited communications with or without human intervention.

Yet again, the serious problem of understaffing, which the HDPA has been going through since its establishment, could not be addressed in the year 2011 due to the well-known current public financial situation.

In addition, the continuous decrease of the budget being granted to the DPA for operational needs restrains the HDPA's ability to sufficiently meet its obligations.

More specifically, the HDPA issued two guidelines: a) Guideline 1/2011 on the use of video surveillance systems for the protection of persons and goods in publicly accessible private areas and b) Guideline 2/2011 on e-consent regarding commercial communications sent by electronic means (see case-law).

The HDPA also gave advice to the government, the parliament and other independent authorities via the following Opinions and Decisions: a) following requests by the Ministry of Finance and the Parliament, the HDPA delivered its opinion on a number of tax issues, concerning in particular the publication of tax data on the Internet (Opinion 1/2011, Opinion 4/2011, Opinion 7/2011, Decision 54/2011 – see case-law), b) the HDPA participated in a legislative Committee of the Ministry of Justice for the incorporation of Directive 2009/136/EC into the national law and the amendment of Law 3471/2006 on the protection of personal data and privacy in electronic communications, c) the HDPA contributed to the public consultation on the draft regulation of the Hellenic Authority for Securing the Secrecy of Communications, an independent administrative authority, d) upon a request by the Hellenic Parliament, the HDPA expressed its views on the "Proposal for a regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System"(the IMI Regulation), e) the HDPA expressed its views to the Regulatory Authority for Energy, another independent administrative authority, regarding the proposed measures for the administration of the debt of the electricity providers' customers.

In addition, it issued Decision 50/2011 on processing requests for extrajudicial settlement by "Tiresias Bank Information Systems S.A.", Decision 52/2011 regarding the census of the population and housing

procedure, conducted by the Hellenic Statistical Authority and Decision 53/2011 regarding the "Google Maps Service" (see case-law).

On the occasion of European Data Protection Day 2011 the Hellenic DPA added a special section to its website to raise awareness among secondary school pupils about the safe use of Internet services. Furthermore, an instructive and self assessment tool was created regarding identity theft, which was aimed at all age groups. The Ministry of Education gave its aid to this initiative by inviting secondary schools to use the material for the benefit of their pupils. In addition, HDPA experts visited selected schools. Finally, a bulletin was published on the website and a press release was issued.

Organisation	
Chair and/or College	Christos Yeraris (Chair) until May 2011 Petros Christoforos (Chair) since August 2011
Budget	EUR 2 339 500
Staff	Auditors Department: 16 lawyers and 11 IT experts (of whom, five (5) on maternity leave, one (1) was seconded for part of the year to the EDPS as a national expert, one (1) on educational leave and one (1) resigned). Communications & Public Relations Department: 5 (of whom, one (1) on maternity and educational leave for half of the year). Human Resources & Finance Department: 16 and one (1) seconded from another civil service.
General Activity	
Decisions, opinions, recommendations	The HDPA issued 168 decisions, 7 opinions and 2 guidelines. Of them 6 decisions, 5 opinions and 2 guidelines have an effect on data protection in general.
Notifications	The HDPA examined 702 notifications (414 of them concerned installation and operation of CCTVs and 70 data transfers to countries outside the E.U.).
Prior checks	The HDPA granted or renewed 63 permits concerning processing of sensitive data, interconnection of files and data transfer to countries outside the E.U).
Requests from data subjects and data controllers	1 011
Complaints from data subjects	812 (Prosecution Authorities and Public Order: 76, National Defence: 2, Public Administration and Local Government: 33, Taxation – Ministry of Finance: 4, Health: 20, Social Security: 9, Education and Research: 5, Banking: 51, Private Economy: 163, e-communications:

	131, Work relations: 25, Mass Media: 7, Other: 286).
Advice requested by parliament or government	9 (Opinion 1/2011, Opinion 4/2011, Opinion 7/2011, Decision 50/2011, Decision 52/2011 – see also section A – summary).
Other relevant general activity information	
Inspection activities	
Inspections, investigations	7 inspections (of them 3: Ministry of Education, 1: National Eurodac Unit, 1: Anti-Money Laundering Authority, 1: social security (online prescription system) and 1: private economy.
Sanction activities	
Sanctions	22 sanctions (18 warnings, 4 penalties) decided by the DPA in following sectors: health care (13,) social security/insurance (2), spam (2), CCTVs (2), telecommunications (1), bank (1), public sector (1).
Penalties	Amounts: EUR 3 000 – EUR 10 000 (total EUR 27 000) were imposed by the HDPA.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Guideline 1/2011

The HDPA issued Guideline 1/2011 on the use of video surveillance systems for the protection of persons and goods in publicly accessible private areas, replacing the previous one. It includes general and specific provisions concerning different categories of controllers. Particular emphasis was laid upon the application of the principle of proportionality.

Guideline 2/2011

The HDPA issued Guideline 2/2011 on e-consent regarding commercial communications sent by electronic means. It defined the procedure for consent given by users to be considered valid, and provided guidance for the controllers as to the procedure and technical means that they should have available for proving the given e-consent.

Opinion 1/2011

An opinion was delivered regarding the lawfulness of two different applications planned by the General Secretariat of Information Systems within the Ministry of Finance for the publication of tax payers' lists on

the Internet. In the first case, the Authority judged that the publication of tax payers' lists in tax offices, municipality offices, in the media and on the Internet for the purpose of combating tax evasion does not conform to the principle of proportionality. Regarding the second application, the HDPA judged that the service of taxpayers' register data validation conforms to Articles 9(a) and 25, paragraph 1 of the Constitution since no information about the income of the taxpayers and the corresponding tax is revealed.

Opinion 4/2011

The HDPA judged that the publication of the list of debtors of overdue payables to the Greek State on the Internet by the General Secretariat of Information Systems within the Ministry of Finance, which, in the current critical public financial situation, the Greek legislator opted for, as an appropriate measure in principle for the fulfilment of citizens' tax obligations to the State, is constitutionally tolerable data processing, not exceeding the limits of the principle of proportionality. In this context, the Authority considered that the aforementioned publication does not contravene the superior rules that safeguard the right of individuals to the protection of their personal data, if certain conditions, that the HDPA defined, are fulfilled.

Opinion 7/2011

The HDPA delivered an opinion on the publication on the Internet of Parliament Members' asset declarations, upon a request by the Greek Parliament. Taking into account the law which expressly stipulates the publication of Parliament Members' asset declarations, including the Parliament's website, the HDPA judged that the limitation of the personal right is provided for in the law, justified by sufficient reasons of public interest, as it serves transparency in political and public life and falls within the limits of proportionality, as it serves superior legal interest.

Decision 50/2011

Upon a question by the General Secretariat of Consumer Affairs the HDPA deemed that data related to the submission of requests for extrajudicial settlement, provided for in the Greek legislation, are lawfully collected by the credit reference agency, TIRESIAS Bank Information Systems S.A. without the data subjects' consent. The credit institutions can access these data only with the data subject's consent when a data subject has applied for a loan.

Decision 52/2011

The HDPA deemed that the national legal framework concerning the census of population and housing procedure, in force at the time of the 2011 census conduct, did not fulfil the conditions set out by the Greek Council of State and the European Court of Human Rights with regard to the limitations of personal rights, as the basic issues relating to the general census of population and housing were not clearly and specifically provided for in any law or presidential decree. Furthermore, the DPA laid down the specifications for the organisational and technical measures required for the security of such data. As a result, the legal void was filled by the Law 3995/2011.

Decision 53/2011

In year 2011, Google Inc., amended its initial notification to the HDPA concerning the "Street View" service, which was pending, with regard to its purpose, appointing also as a local representative, Google Greece Applications Ltd. The company declared the road mapping of Greek areas as the new sole purpose, which would also be used for other relevant services, such as navigation services. The HDPA considered that the "Google Maps" service entails processing of personal data to the extent that the pictures taken include faces, vehicle licence plates and houses. This processing is lawful, according to the data protection law, since the deployment of economic activity constitutes in principle a lawful purpose. Nevertheless, given that the data subjects, who may directly or indirectly be identified from the pictures, have had no prior contractual or any other relationship with the controller, the service must be provided under certain conditions, as following: a) permanent blurring of pictures of faces, licence plates and houses within one year from the day the pictures were taken, b) adequate organisational and technical security measures for the protection of raw data, c) measures to avoid the collection and further processing of images that might reveal sensitive personal data, d) adequate prior notification to the public by means of appropriate press and website announcements, and e) fulfilling the right of access, provided that the data subject submits adequate information for locating the data relating to him/her.

Decision 54/2011

The HDPA judged that the publication, on the website of the Ministry of Finance, of lists of doctors who had allegedly evaded tax, wasn't provided for in the law. On the contrary, the publication contradicted a legal provision establishing tax secrecy, which can be by-passed only in cases provided for in specific legal provisions. The Authority concluded that the publication constitutes an unlawful data processing and addressed a warning to the controller to cease the processing within fifteen (15) days and remove the specific press release from the website of the Ministry of Finance.

HUNGARY

A: Summary of activities and news:

The Parliamentary Commissioner for Data Protection and Freedom of Information, as the responsible DPA of 2011 did not compile an annual report or a cumulative statistical data base on his 2011 activities. The National Authority for Data Protection and Freedom of Information – set up in January, 2012 – provides the below figures for 2011 on the basis of registers produced by the Commissioner's office.

Organisation	Parliamentary Commissioner for Data Protection and Freedom of Information
Chair and/or College	Dr András Jóri
Budget	HUF 352 381 000
Staff	49
General Activity	
Decisions, opinions, recommendations	5 461 (number of cases, including data protection registry notifications) 71 recommendations are available on the official web page of the Parliamentary Commissioner from the year 2011.
Notifications	N/A
Prior checks	14 (all related to data protection registry notifications).
Requests from data subjects	3 162 (data protection registry notifications).
Complaints from data subjects	949
Advice requested by parliament or government	290 (opinions given on draft law related to either data protection or freedom of information issues).
Other relevant general activity information	797 consultations, 112 international related cases (related to either data protection or freedom of information issues).
Inspection activities	
Inspections, investigations	309 (in connection with completed and justified complaints).
Sanction activities	
Sanctions	Parliamentary Commissioner was not authorised to issue.

Penalties	Parliamentary Commissioner was not authorised to issue.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Two important examples:

a) *Unlawful data processing – provider of website* (www.ingatlandepo.com and www.ingatlanbazar.com)

The Data Protection Commissioner (hereinafter referred to as DPA) investigated the case of a website provider company (hereinafter referred to as data controller). Contracts were concluded between Hungarian data subjects and the data controller with the purpose of advertising real estate on behalf of the data subjects on the website of data controller.

Once the real estates were sold, the advertisements expired or the data subjects simply wished to delete – or get them deleted by the data controller – their ads. They failed to do so. Despite their strong and repeated requests the data controller failed to delete the advertisements. Moreover the data controller passed on the personal data of the data subjects to – among others – claim management companies.

Numerous complaints were received by the DPA with respect to the above issues. As a result the DPA launched an investigation procedure and called the data controller to make statements on its behaviour within a certain period of time.

As a result of the procedure, the DPA concluded that the data controller had violated the privacy rights of the data subjects on multiple counts. Among others the data controller infringed the principle of proportionality, the right for information, the right of the data subjects to delete their personal data or to have them deleted by the data controller, as well as the principle of purpose limitation. Additionally the data controller neglected the multiple objections made by the data subjects in line with the data processing of the data controller. Therefore the data controller lacked the essential legal basis for various data processing activities.

As a consequence the DPA issued a press release and a statement affirming that the onward disclosure of real estate advertisements, implying also the processing of personal data, in spite of the explicit will of the clients, qualified as unlawful. Furthermore these methods cannot be used as a sanction in order to recover a claim against the clients. The DPA called the clients' attention to thoroughly consult the privacy policy of the service provider prior to rendering their personal data.

b) Biometric identification relating to public bath entry passes

A client, in his submission, requested the DPA to deliver an official statement as to whether the data processing of a public bath/spa operator could be lawful where the operator intends to install a biometric identification system at entry passes. According to the intentions of the operator the biometric system would store the fingerprints of customers thus enabling a more effective and customer-tailored identification system for the service provider.

In his/her submission the client enquired if fingerprints qualify as personal data that may be controlled upon the data subject's consent. Additionally the client asked whether there are more specific – eventually stricter – rules in effect governing the data processing of fingerprints.

Considering the relevant national and EU regulations the client was advised as follows:

Fingerprints of a natural person qualify as personal data and the taking, as well as storing; of fingerprints qualify as data processing. Not only the relevant national legislation but also the EU Data Protection Directive stipulates fundamental legal principles which should also be regarded in data processing activities. These include – among others – the principle of proportionality and necessity.

The Data Protection Working Party (WP 29) emphasised the need for inspection as to whether the operation of the biometric ID system is necessary to achieve the goals set by the service provider. In this respect the following aspects shall be thought over:

- Whether the installation of such a system is either indispensable or simply cost-effective and comfortable;
- Whether the operation of such a system will be effective, and if so, to what extent;
- Whether the restriction of privacy is proportional to the predictable advantages;
- Whether the goals set by the service provider could be achieved by less restrictive means.

Finally, as a conclusion, the DPA found that a biometrics system – aimed at taking and storing fingerprints of clients upon entering the public bath/spa complex – for the purpose of a better and more effective personal identification does not meet the requirements of proportionality. Better identification, instead, could be secured by any other – more harmless and less restrictive to privacy – way, e.g. entry passes with photos etc. Consequently the introduction of such an entry system would not comply with the data protection rules.

C. Other important information

Major legislative changes in Hungary

As a result of fundamental changes in the constitutional structure of Hungary, following a decision of the Hungarian National Assembly in 2011, the functioning of the former Data Protection Commissioner's Office was terminated and the establishment of a new body called the National Authority for Data Protection and Freedom of Information tasked with the responsibilities mentioned previously was expected to commence its work on 1 January 2012. The new legal instrument intended to govern the field of data protection and freedom of information, Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information was adopted by the Parliament on 11 July 2011.

IRELAND

A. Summary of activities and news:

The Office of the Data Protection Commissioner opened 1 161 formal complaints for investigation in 2011 (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 17 complaints giving rise to formal decisions. Information in regard to prosecutions in 2011 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 1 458 000 (EUR 1 516 404.20)
Staff	20
General Activity	
Opinions, recommendations	3 (Guidance).
Notifications	There were approximately 5 000 registrations in 2011.
Prior checks	None
Requests from citizens	15 000
Complaints from citizens	1 161 (access rights – 48%, electronic direct marketing – 22%, disclosure – 10%, unfair processing – 10%, other – 10%).
Advice requested by parliament or government	>100
Other relevant general activity information	1 167 personal data security breach notifications from 186 different organisations.
Inspection activities	
Inspections	28 audits (inspections).

Sanction activities	
Sanctions	54 prosecutions in 2011 against 6 entities.
Penalties	EUR 15 400+ costs (fines/settlements imposed by courts).
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In the course of 2011, 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). Six entities were prosecuted for various offences in 2011.

C. Other important information

Transposition of the ePrivacy Directive

On 1 July 2011, Ireland transposed the revised ePrivacy Directive by way of SI 336 of 2011.

The Regulations introduced a mandatory data breach notification requirement for electronic communications networks and providers. It also set a high bar for all such entities in relation to the security measures which they must take to protect personal data for which they are responsible. They must, inter alia, ensure that such personal data is secured and only available to approved personnel on a need-to-know basis. Failure to comply can result in a criminal prosecution with summary fines of up to EUR 5 000 and an indictment of EUR 250 000 per offence.

The opportunity was also taken in the new law to clarify a number of matters in relation to direct marketing contact with consumers. Perhaps of most interest is that prior consent is now required to phone a person on their mobile phone for a marketing purpose unless that number is recorded as willing to receive marketing calls on the National Directory Database (NDD) – there are twelve such numbers so recorded as of 13 March 2012!

Also of interest is that a non-marketing SMS message may not have marketing material "tagged on" unless the recipient has given prior consent to the receipt of such messages. Also the requirements are extended to all forms of marketing carried out by means of a publicly available electronic communications service – including, for example, the soliciting of support for charitable organisations or political parties.

ITALY

A. Summary of activities and news:

News, Changes in the Laws:

Significant amendments were made to the Italian DP Code in 2011. They mainly concerned the following:

- Processing of personal data relating to legal persons: The Act containing urgent financial measures (May 2011) excluded legal persons from the scope of application of the DP Code, if the processing was performed for the so-called administrative and accounting purposes and as part of business-to-business relations (see Section 5(3) of the DP Code). Whilst this provision was subsequently repealed (in December 2011), a new amendment to the Code (Section 4), introduced in May 2012, ultimately excluded legal persons from the definition of "personal data" – whereby a personal data is "any information relating to a natural person" only. This means that the DP Code currently does not apply to the processing of personal data relating to legal persons (including associations, foundations, committees, etc.); however, the DPA issued a detailed opinion (published ultimately in October 2012) to clarify that this is to be construed not to exclude legal persons to the extent that they are "subscribers" to a publicly available electronic communications service as per the definitions contained in the DP Code in pursuance of the e-privacy Directive (Section 4(2)f.);

- Telemarketing: The 2011 Act on urgent financial measures also extended the opt-out regime to unsolicited postal marketing alongside telephone-based marketing. Based on the latter amendment, direct marketers may now rely on postal addresses contained in subscriber directories without having to obtain the subscribers' prior consent – providing such subscribers have not opted out of this promotional activity by entering their phone numbers and postal addresses in the ad hoc Opt-Out Register;

- Security Policy Document: A further instance of simplification was introduced via the said 2011 Act to exempt "an entity [that] only processes non-sensitive personal data or else sensitive and judicial data that relate to the respective employees and collaborators, including non-EU nationals, and/or to their spouses and/or relatives" from submitting the so-called "Security Policy Document" (*Documento programmatico per la sicurezza*, DPS) to the DPA. This obligation was repealed altogether via an amendment to the DP Code that was introduced in May 2012. It should be recalled that all the other security measures continue to be fully applicable;

- Additional amendments were made by the 2011 Act, which exempted private entities and profit-seeking public bodies from obtaining prior consent in order to process personal data contained in CVs or biographies if these are sent voluntarily by prospective job candidates as well as in order to transfer personal information within a corporate group.

Key Areas of Activity in the course of 2011:

Journalism and Online Information: Whilst acknowledging that the publication of court transcripts is no longer subject to confidentiality constraints is part of freedom of expression, the DPA issued an injunction to a website banning online dissemination of information that was excessive as well as irrelevant for the specific information purposes – even though it was contained in the judicial order to remand the defendant in custody.

Genetic Data: The general authorisation granted by the DPA to process genetic data was upgraded following an opinion rendered to the Italian Ministry of Health. The new general authorisation takes account of the experience gathered as well as of the contributions coming from authoritative experts; it was also granted to public and private mediation organisations as per the legislation enacted recently.

Processing for Purposes of Scientific Research: In 2011 there was an upsurge in the applications to authorise processing for purposes of scientific research without the data subjects' consent, on account of the alleged impossibility to inform a significant portion of the patients concerned. The DPA issued a provisional general authorisation taking account of the most frequent cases in which one could justifiably fail to inform data subjects – in particular because of "ethical reasons" and/or "impossibility resulting from organisational arrangements".

Processing Data in the Employer-Employee Relationship: Several decisions issued in 2011 highlighted the multifarious situations in which employer-employee relationships develop along with the need for carefully considering the relevance of any personal information used in this context. The main decisions concerned monitoring of employees' Internet navigation; admissibility in disciplinary proceedings of information retrieved from the web; use of questionnaires on employees' personality traits; disclosure of information on alleged "moonlighting" (second jobs) to the national occupational insurance body; geolocation of employees; etc.

Telemarketing: The DPA clarified that the roles played by the entities involved in telemarketing activities should be determined by having regard to the factual circumstances in which the processing of personal data takes place. In principle, the data controller is the entity on whose behalf and/or in whose name the promotional activities are being implemented; accordingly, the Italian DPA specified that any company outsourcing its promotional activities to external providers whilst retaining the factual operational control over such activities must appoint the promoters, agents, etc. in question formally as data processors in compliance with the Italian DP law.

Unsolicited marketing calls, following the setting-up of the "Opt-Out (Do-Not-Call) Register" for users that do not wish to receive promotional calls, in the light of the relevant implementing difficulties;

"Silent" calls, i.e. those phone calls – at times repeated on the same day – in which users are left without any safeguards and remedies to face the "dead air" on the caller's side. In this connection, the DPA ordered a company that relied on a dialer-based system to implement various arrangements and measures in order to prevent repeated silent calls and rule out the calling of the same number for at least a 30-day period;

Unsolicited faxes: The DPA ruled that the Italian DP Code applied to a company established in a third country that kept (prospective) customers' personal data in such country and relied on remote data handling mechanisms, to the extent that the company made use substantially of a data transmission equipment (fax gateway) located in Italy. For this reason, the promotional faxes sent by the said company without providing suitable information notices and obtaining the recipients' prior consent were found to be unlawful and accordingly prohibited.

Telephony: The main areas of activity in this case are related to the "Online subscriber directories": several complaints had been lodged against a company that had posted a subscriber directory including "confidential" information on the web. The DPA found the processing in question to be unlawful insofar as the personal data contained in the directory had not been taken from the "Unified Telephone Database" (DBU, Database Unico), which is the only legitimate source for telephone subscriber directories under Italian law.

Relationships with Parliament and Other Institutions

The DPA was heard by Parliament on several occasions before Parliamentary Committees or other Parliamentary Forums on issues tabled by Parliament as well as in connection with fact-finding initiatives or prior to the passing of bills. In all cases the DPA pointed out the possible implications for the processing of personal data. Reference can be made in particular to the following:

Bills containing provisions to enable implantation of unused embryos kept at Italian centres for medically assisted reproduction;

Amendments to the Italian Data Protection Code (see above); additional relevant provisions contained in Decree No 70/2011 (urgent financial measures),

Operation of the national unified coding system as used in connection with the comparative study on effectiveness, quality and appropriateness of Italian health care agencies;

Fact-finding investigation into degenerative diseases of special social importance, with particular regard to breast cancer, chronic rheumatic diseases and the HIV syndrome.

Considerable importance should be also attached to the opinions rendered by the DPA concerning both secondary legislation (Government-initiated instruments) and regional legislation impacting the protection of personal data (under Section 154(4) of the DP Code). Mention can be made of the Opinions regarding the Register of mammal prostheses; a regulation laying down technical rules for implementing ICT in civil and criminal proceedings; technical rules to identify the owner of a certified email account also via electronic networks; management of the Register of auditors and auditing companies; the Guidelines issued by Digit-PA [the public agency in charge of fostering ICT in the public administration] regarding disaster recovery in the public sector; the provisions supplementing Italy's civil procedure code as for reducing and simplifying fact-finding proceedings under civil law. However, it should be pointed out that the DPA was not asked for the advice mandated by the law in all cases in which data protection issues were involved.

The International Dimension

As well as contributing actively to the work done by the Article 29 Working Party, the Italian DPA continued following the developments related to the European data protection reformation – in particular via contributions to the Future of Privacy subgroup of the WP29 on simplified notification requirements, the processing of personal data and cooperation among European DPAs. The Italian DPA is also participating actively in OECD working groups that deal with privacy and data protection issues (in particular the Working Party on Information Security and Privacy – WPISP) as well as in the Council of Europe's T-PD Advisory Committee and Bureau (which is currently working on a revision of the 108/1981 Convention). The DPA is a member of joint supervisory authorities competent for checking on the operation of shared information systems (Europol JSB, Schengen JSA, CIS, Eurodac co-ordination group). Mention should also be made of the activities related to the so-called Berlin Group (International Working Group on Data Protection in Telecommunications), where it was co-rapporteur of the Working Document on the right to privacy and right to oblivion on the web, and of the contribution provided to the discussion within the Case Handling Workshop of European DPAs. As for judicial and police cooperation in criminal matters, the DPA continued its activities in support of the WPPJ (Working Party on Police and Justice) – chaired by its President, Professor Pizzetti – until the latter Working Party was terminated.

Other Areas of Activity

The DPA continued its awareness-raising initiatives by focusing especially on youths; to that end, ad-hoc publishing initiatives were launched concerning social networks, schools and health care. A competition was also organised, called Privacy 2.0: Youths and New Technologies, in which secondary school students were called upon to create short films on privacy and thus work as script-writers, performers, directors, and so on.

Organisation	Garante per la protezione dei dati personali
Chair and/or College	Chair: Prof. Francesco Pizetti College: Giuseppe Chiaravalloti Mauro Paissan Giuseppe Fortunato
Budget	Approx. EUR 8.5 million (funding by Government)
Staff	123
General Activity	
Decisions, opinions, recommendations	Number of decisions taken by the College: approx. 540
Notifications	1 218
Prior checks	22
Requests from data subjects	Total number of requests: approx. 4 450 Requests for information (*quesiti*): 332 Reports and claims (*segnalazioni* and *reclami* received in 2011) from data subjects: 4 022
Complaints from data subjects	(Formal complaints, specifically regulated by the DP Code, concerning access to one's personal data) Approx. 260
Advice requested by parliament or government	Opinions in reply to parliamentary inquiries: 4 Opinions to Ministries and to the PM Office: 32 Topics: police, public security: 2 Judicial activity: 2 E-government and databases: 8

	Education and training: 3 Employment in public bodies: 2 Health care: 6 Businesses: 5 Welfare: 2 Registrar of births, death, marriages: 2
Other relevant general activity information	The front office of the DPA received, in 2011, about 32 000 telephone calls and emails. National authorisations for BCR: 1
Inspection activities	
Inspections, investigations	Number of inspections and/or investigations (on the spot): approx. 450 (in 37 of which infringements having a criminal nature were reported to the judicial authority).
Sanction activities	
Sanctions	Approx. 400
Penalties	Amount: approx. EUR 3.1 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

Relationship between right of defence and protection of privacy

A decision by the Court of Cassation dated 8 February 2011 was much debated. The case in point concerned the transfer – more accurately, the unlawful dissemination – of personal data held by a lawyer who had kept the records concerning his client even after termination of the retinue agreement, because he had not yet been paid his fees. The records in question also included sensitive information. The Court ruled that it was necessary to take due account of "the actual features of the relationship between data collection and the underlying purpose(s)"; here, the data at issue had been collected "to establish or defend a legal claim". However, the lower court ought to have established whether all the data held by the lawyer

were *de facto* necessary to defend the claim vested in the lawyer *vis-à-vis* his client. In short, the Court of Cassation affirmed the need to abide by the principles of fairness, relevance and non-excessiveness of data as set forth in the DP Code and confirmed that whoever holds sensitive information concerning another may in no case disseminate such information (which would carry the punishments mentioned in Section 167 of the DP Code).

The same stance was taken by the Court of Cassation (Criminal Law Division) in a judgment of 24 March 2011. In the Court's view, "disclosing a recorded conversation for purposes other than protecting one's own or another's right" amounts to the criminal offence that is punished under the terms of Section 167 of the DP Code. In the case at issue, the conversation had been recorded by a private detective using a pen that contained a microphone and a micro-camera, which were invisible to the other parties.

Regarding the relationship between freedom of information rights as exercised with a view to defending a legal claim and personal data protection legislation, the prevailing stance in case-law would appear to be that freedom of information rights override conflicting interests as expressly provided for in the law (in particular, the legislation on freedom of information). More specifically, freedom of information rights override third parties' rights to privacy even if sensitive information is at issue. This view was supported by various administrative courts: Regional Administrative Court of Tuscany, judgment of 12 May 2011; Regional Administrative Court of Liguria, judgment of 1 June 2011 – where it was ruled that "protecting the right to privacy is no sufficient reason to reject the request for producing whatever documents"; Regional Administrative Court of Lombardy, judgment of 1 August 2011.

Surveillance in the Employment Context

In a decision of 22 March 2011, the Court of Cassation (Labour Law Division) ruled that if audio-visual devices are installed in a company upon prior agreement with the competent trade union representatives, any recordings showing an employee's conduct to be such as to justify the latter's dismissal (because of the theft of corporate assets) may be used in the judicial proceedings concerning the relevant matters. Furthermore, a decision by the Court of Cassation (Criminal Law Division) of 9 August 2011 clarified that recordings performed by the police inside the premises of a health care unit were admissible as evidence in trial as they showed that an employee had tampered with the clock-in procedure. The complainant's view was that the workplace could be equated to one's home, whereupon any audio-visual recording had to be authorised and justified by the competent judicial authority. The Court clarified that the concept of "home" refers to a peculiar relationship with a place in which an individual's private life is conducted in such a way as to prevent that individual's exposure to external interference under any circumstances. Conversely, this does not apply to the premises of a public office irrespective of whether such office was the workplace of the defendant, and this is even less so in the case of the entrance to the premises of a health care unit – which is a transit area for all the employees as well as for all the users of health care services.

Privacy and Journalism

In a judgment of 28 September 2011, the Court of Cassation (Civil Law Division) upheld a judgment by an Appellate Court which had ruled out any harm coming from publication of a newspaper feature since the facts at issue had been demonstrated to be true. In the Court of Cassation's view, no harm is caused to an individual's identity if a newspaper feature only reports factual circumstances that have occurred in reality.

LATVIA

A. Summary of activities and news:

A major development in 2011 was related to a new function that has been entrusted to the Data State Inspectorate of Latvia – in order to ensure the implementation of Directive 2009/136/EC regarding data breach notification. Amendments to the Electronic Communications law were elaborated (in force since 8 June 2011) but this function has been entrusted to the Inspectorate without additional resources, which causes a major challenge for the Inspectorate.

In 2011 the processing of sensitive personal data was determined as the priority where preventative control activities also occur (for example, regarding the processing of medical data, use of video surveillance in hospitals and special social centres). 30% of all the prior checks were carried out regarding data processing in the health sector. As a result of the control activities, the following was concluded, that in many cases:

1. There were no internal procedures for data protection in place, and data protection audits had not been carried out;

2. Access rights were not determined according to the duties of employees;

3. The control activities regarding access rights were not in place.

The work of data protection officers was also supervised as the number of the officers has a general tendency to increase in Latvia. As an alternative to the notification, since 2007 the controller can designate data protection officers. There were no major shortcomings concluded regarding the work of data protection officers. Until the end of 2011 there have been 40 persons who have passed the exam in Data State Inspectorate and have obtained the certificate of data protection officer.

Regarding public awareness – there was a recommendation issued for child data protection. This recommendation has been widely used by the staff of schools and pre-schools. The Data State Inspectorate provided several seminars for teachers, directors of schools and other administrative staff regarding personal data protection issues, covering both the data protection of pupils and school employees. It has been acknowledged by the target audience that such practical recommendations are very useful.

Public awareness activities were carried out also in cooperation with other state institutions (for example CERT.LV) in order to promote an understanding of privacy and data protection issues. It is foreseen to continue this cooperation also in 2012.

Organisation	Data State Inspectorate
Director	Signe Plūmiņa
Budget	LVL 266 907 (approximately EUR 368 656.08)
Staff	19 (including administrative staff).

General Activity	
Decisions, opinions, recommendations	1 recommendation. No statistics available regarding Decisions and Opinions. Opinions are issued regularly regarding draft legislation.
Notifications	650.
Prior checks	Statistics will be available starting from 2012.
Requests from data subjects	
Complaints from data subjects	254
Advice requested by parliament or government	Regularly, both regarding the implementation of specific legal acts and problems related to data protection issues.
Other relevant general activity information	
Inspection activities	
Inspections, investigations	290 investigations carried out.
Sanction activities	
Sanctions	Both warnings and fines have been applied.
Penalties	In amount of LVL 23 100 (EUR 31 906.08). Fines applied both for illegal actions as well as for not providing information to the Data State Inspectorate.
DPOs	
Figures on DPOs	40

B. Information on case-law

The economic situation in the country influences the complaints received in the Data State Inspectorate regarding personal data processing. Mainly the complaints were related to the following issues:

1. Information provided by employers to the State Revenue Service on employed employees without an employment relationship (thus data subjects could not receive any social benefits from the State as there was an employment relationship in place of which they were not aware).

2. Personal data processing within the debt collection process.

3. Personal data processing within video surveillance.

4. Publishing personal data illegally on the Internet.

LITHUANIA

A: Summary of activities and news

The law amending and supplementing the Law on Electronic Communications (Official Gazette, 2004, No 69-2382) (hereinafter – LEC) came into force on 1 August 2011, implementing into Lithuanian law the provisions of the e-Privacy directive.

On 4 May 2011 the Government of the Republic of Lithuania adopted Resolution No 522 "On implementation of Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes". According to Article 1.2 of this Resolution the SDPI was appointed as a supervisory authority responsible for the independent supervision of data entered into the Customs Information system.

On 9 November 2011 the Government of the Republic of Lithuania adopted Resolution No 1324 "On the approval of the procedure for the cross-border exchange of DNA data, dactyloscopic data, data of vehicle registration, their owners and possessors and information related to large-scale cross-border events or terrorist crime prevention", by which the SDPI was appointed as responsible for the legality checks for personal data disclosure and receiving.

On 17 June 2011 the Director of the SDPI issued an order, "On the approval of the Procedure for the implementation by the data subject through the State Data Protection Inspectorate of the data subject's rights of access to their personal data, and to rectify, erase or block such data" implementing the Law on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters.

On 22 July 2011 Director of the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI) issued an order, "On approval of procedures for personal data security breach notification". By this order the personal data security breach notification procedure and the form on data breach notification were approved, giving guidance on how data breaches shall be notified. In addition several workshops for service providers were organised.

For the practical implementation of requirements of e-Privacy directive on cookies the SDPI, Ministry of Justice and Ministry of Transport and Communications started an initiative on the implementation of these into websites of Governmental institutions and municipalities, and discussions on how to make recommendations were prepared by the SDPI mandatory.

European Data Protection Day was celebrated on the 27 January 2011. Press conference and activities at the Seimas of the Republic of Lithuania on the topic "Privacy in cyberspace" were organised. On 10 February 2011, Data Protection Day was commemorated at Vilnius University. The aim of the day was to give better understanding of threats to personal data security while processing data in cyberspace (social networks, Google, credits by Internet and other electronic channels). The main target group was students of universities and colleges.

The SDPI, together with a joint stock company, Expozona, organised a conference "Data protection in Lithuania: updates, problems and perspectives" on 19 May 2011. The event focused on the use of technologies and the provision of data from registers, and was devoted to companies, institutions and organisations, managers, lawyers, professionals responsible for the personal data processing of employees and customers.

In addition, the SDPI again with a joint stock company, Expozona, organised a conference "Data protection in Lithuania: innovations, updates and problems" on 24 November 2011. This event was focused on the legal aspects of the protection of personal data: to present amendments of the Law on the Legal Protection of Personal Data of the Republic of Lithuania, important court decisions, discussing the problems of the jurisdiction and other issues.

Organisation	
Chair and/or College	Dr Algirdas Kunčinas
Budget	Allocated and executed LTL 1 881 million (EUR 546 484)
Staff	30
General Activity	
Opinions, recommendations	N/A
Notifications	998
Prior checks	257
Requests from citizens	14
Complaints from citizens	256
Advice requested by parliament or government	N/A
Other relevant general activity information	3 356 consultations; 88 public information releases; 6 summaries on the results of the complaints investigation and case-law; 5 requests on data processing in the C.SIS; 63 conclusions on EU and Council of Europe documents; 82 responses to inquiries from parties of the Convention (ETS No 108); 234 coordinated legal acts and data controller documents; 6 prepared legal acts.
Inspection activities	
Inspections	43 (Internet traffic data storage legitimacy, when providing Internet services; data processing legitimacy, scope and data subject rights in Internet shops).
Sanction activities	
Sanctions	The SDPI drew up 24 protocols for administrative violations.
Penalties	N/A
DPOs	

Figures on DPOs	N/A

B. Information on case-law

Processing of a debtor's personal data

The SDPI received a complaint alleging that a debt collection agency, having obtained the complainant's personal data from the initial creditor from a cession agreement, illegally transmitted that personal data to the consolidated debtor's file. The SPDI found that the complainant had not contested the debt on compelling grounds and concluded that the complainant's personal data was communicated to the consolidated debtor's file legally. The complainant appealed the decision of the SDPI to the Vilnius district administrative court, on the grounds that the SDPI had not specified why the complainant's contest had not been on compelling grounds. The Vilnius administrative court overturned the decision of the SDPI and ordered the SDPI to reinvestigate the case. The SDPI appealed this court decision to the Supreme Administrative Court.

The Supreme Administrative Court (hereinafter – Court) assessed that the Law on the Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – LLPPD) does not provide a definition of compelling grounds, and consequently there is no basis to conclude that a person, who has once challenged the debt must continue to do so regularly, failing which, after subsequent written reminders from the data controller, his data can be transferred to the consolidated debtor's file after 30 calendar days from the last reminder (Article 21, paragraph 2.3 of the LLPPD). In deciding how the term "compelling grounds" should be understood, the Court took into account several aspects including whether or not the data subject had reasonably challenged the controller, in this case the creditor, as to the assessment of the evidence on which its decision is based; and in the absence of agreement, one party cannot make a decision binding on the other party. The SDPI appeal was rejected, and the decision of the Vilnius district administrative court left unchanged.

LUXEMBOURG

A. Summary of activities and news

Legislative changes

The law of 28 July 2011 implements the provisions of Directive 2009/136/EC into Luxemburgish law, via a modification of the law of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications. It provides for a definition of a "data breach" and obliges a mandatory notification of the DPA in case of every breach, as well as a notification of the concerned persons, if the latter are negatively affected by the breach. An important evolution under Luxembourgish law constitutes the right to fine the data processor, in case of recurrent data breaches. The law also modifies some minor provisions in the law of 2005, as well as the modified law of 2 August 2002.

Key topics

The *Commission nationale* did advise the Luxembourgish government on a vast array of legislative topics during 2011, among which the most important was the draft law implementing a national pupil database held by the Ministry of Education. The Luxembourgish DPA has continued to work with different Ministries and public administrations on projects that have an impact on privacy like, for example, electronic health records, the reform of the criminal record, the introduction of a biometric residence permit and the European citizens' initiative.

News

The CNPD has concluded a contract for strategic partnership with the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg. The joint research programme includes three main areas: the new European Union legislation initiatives in the field of data protection, the new technological challenges like cloud computing and their implications for Luxembourg and the concept of "privacy by design".

Key events and awareness raising

The CNPD celebrated the European Data Protection Day by organising the conference, No privacy online anymore?, with Dr Alexander Dix (Berlin Commissioner for Data Protection and Freedom of Information). Richard Allan of Facebook also participated in this conference, which was followed by a round table with political and youth protection representatives. In addition to this event aimed at the general public, the CNPD also participated in multiple seminars and training courses in order to raise awareness among a more specialised public.

Organisation	Commission nationale pour la protection des données (CNPD)
Chair and/or College	Mr Gérard Lommel – President Mr Thierry Lallemang – Commissioner Mr Pierre Weimerskich – Commissioner
Budget	EUR 1 494 000
Staff	College: 3 Legal department: 4 Notifications and prior checks: 2 General administration: 3 Communication and documentation: 1 Total: 13
General Activity	
Decisions, opinions, recommendations	492
Notifications	401
Prior checks	429
Requests from data subjects	314
Complaints from data subjects	115
Advice requested by parliament or government	14
Meetings and consultations (public/private sector)	140
Information briefings and conferences	15
BCRs as lead DPA	2
Inspection activities	
Inspections	17
Sanction activities	

Sanctions	0
Penalties	N/A
DPOs	
Figures on DPOs	Designated DPOs during 2011: 10 Total of DPOs designated (at date of report): 48

B. Information on case-law

Civil and criminal case-law

Court of Appeal of Luxembourg, 8th labour chamber on the proportionality and legitimacy of an employee's surveillance at work, 3 March 2011

An employee was suspected of unfair competition practices. He was fired on the basis of a document found on the computer of another employee constituting the former employee's plan to create a competing company. This document was sent from the fired employee's private email account to his colleague's private email, but was saved on the machine of the employer. The Court of Appeal held that the interception and transmission of this document did not constitute a breach of the correspondence confidentiality principle. The Court took into account the fact that said email was addressed to a few employees and that it did not contain any mention that it was private or privileged.

MALTA

A. Summary of activities and news

During the period under review, this Office took legislative measures to introduce amendments to Subsidiary Legislation 440.01 which regulates the processing of personal data in the electronic communications sector. These amendments were required to transpose the provisions contained in Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending, inter alia, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The amendments were introduced by virtue of Legal Notice 239 of 2011, published in the Government Gazette of 24 June 2011. The regulation is expected to be brought into force in 2012 and will also be supplemented by a set of guidelines intended to provide data controllers with the necessary information concerning the implementation of the new requirements, particularly on data breach notifications and the use of cookies.

Data controllers submitted requests for prior checking concerning the introduction of biometric systems and the installation of CCTV camera systems in the workplace and also in other areas where the processing operations involved particular risks of proper interference with the rights and freedoms of data subjects in terms of Article 34 of the Data Protection Act. Further to a request received from the Ministry of Foreign Affairs regarding the processing of biometric data as part of the new VIS, this Office evaluated the relevant data protection implications before authorising similar processing established by Regulations EC 767/2008 and EC810/2009. This evaluation occurred in a meeting with stakeholders and two onsite visits to examine the functionalities of the system and how the national part will be implemented.

In November, this Office carried out two on-the-spot inspection visits in Russia and Egypt at the Maltese Consulates in Moscow and Cairo. The purpose of both inspection visits was to assess the processing of personal data undertaken by both missions in the process of issuing visas for third country nationals. In addition, the visit was carried out with the objective of reviewing certain established procedures in the light of the requirements deriving from the provisions of the Data Protection Act and other legal instruments. A training session on data protection awareness was delivered to members of staff to create awareness on the privacy rights that citizens enjoy under the Act, the relative VIS regulations and the Schengen Convention in relation to the issuing of visas.

On 28 January, the Office of the Information and Data Protection Commissioner joined other Data Protection authorities across the globe to celebrate Data Protection Day. To mark the Day on the local level, the Office distributed informative material and stationery items to students in all state, private and church schools. It has always been this Office's firm belief that for an effective culture change to happen there needs to be continuous investment in educating and raising awareness among the young generation.

With the ever-increasing availability of social networking applications and the consequent blurring of privacy boundaries the Office, by means of this activity, sought to convey a message highlighting the privacy risks data subjects encounter online. This year's message related to the use of Internet and the importance of being aware of the potential privacy risks that the individual's personal data might be exposed to, when made available on the Internet. The Office stressed that the data subject's identity is valuable and therefore it is imperative to keep it safe.

Other awareness-raising activities which were carried out by this Office during the year under review included the delivery of presentations to various data controllers in different sectors of Maltese society, participation in local TV and radio programmes with phone-ins and the regular updating of the Office's portal with developments occurring in the field of data protection. The Office firmly believes that getting the message across via the media, represents a potential and effective way to increase awareness with the public at large.

Organisation	
Chair and/or College	Information and Data Protection Commissioner
Budget	Approximately EUR 300 000
Staff	Commissioner – 1 Professional Staff – 3 Technical Support – 2 Administrative Support – 3
General Activity	
Decisions, opinions, recommendations	38 decisions were issued in relation to complaints received by the Commissioner. 26 opinions/recommendations were issued which related to opinions issued in the form of newspaper articles which were intended for both the general public and data controllers, and other opinions/recommendations provided to data controllers on specific matters.
Notifications	154 new notifications were received.
Prior checks	5 prior checking requests were received.
Requests from data subjects	Queries received by phone – an average of 7 daily calls. Queries received by email – 135.
Complaints from data subjects	70 complaints
Advice requested by parliament or government	N/A
Other relevant general activity information	N/A
Inspection activities	

Inspections, investigations	17 inspections were carried out relating to: investigations of complaints received from data subjects, Maltese consular offices abroad and law enforcement authorities as part of coordinated exercises by the JSA.
Sanction activities	
Sanctions	Court proceedings initiated against a data controller who failed to comply with the orders given by the Commissioner in his decision.
Penalties	N/A
DPOs	
Figures on DPOs	15 Personal Data Representatives were appointed.

B. Information on case-law

No case-law is available for the period under review.

NETHERLANDS

A: Summary of activities and news:

The Dutch DPA supervises compliance with the legislation on the protection of personal data. The Dutch DPA in general focuses on strategic enforcement in order to achieve a higher level of overall compliance. When necessary, sanctions are used.

Priorities are determined on the basis of a continuous risk assessment, for which we use the signals that we receive from various sources in society via different means, such as phone calls, emails and media reports, etc. In 2011, a new signal registration system was introduced that enables us to register signals by sector. The risk assessment takes into account the seriousness of the alleged offence, the number of individuals affected, the clarity of the indication of the breach and the legal feasibility of an enforcement action, as well as the effects of the large-scale use of new technologies. Key focus points for the Dutch DPA in 2011 were, among others: consent, data security, purpose limitation and data retention periods.

An example of the many investigations which Dutch DPA undertook in 2011 is one that deals with youth criminality in the so-called *Veiligheidshuizen*[15] where law enforcement authorities and social welfare institutions work together to prevent and repress criminal behaviour. The outcome of the investigation was that personal data of children under 12 were collected by and exchanged among all the involved parties in regular meetings. However, the *Veiligheidshuizen* were not able to demonstrate on which criteria personal data were exchanged. Moreover, the exchange of the data was not in line with the purpose of the regular meetings and therefore in contradiction with the law. During the enforcement phase of the investigation by the Dutch DPA, the *Veiligheidshuizen* changed their policies and drafted criteria for the exchange of personal data in the meetings.

The Dutch DPA also conducted investigations into, among others, the following data processing operations:

- The exchange of personal data of students (for example: country of birth and race);
- The linking of personal data without consent by the Social Information and Search Service;
- The exchange of personal data by the Dutch tax authority to about 900 help and information desks without verifying the authorisation of the requesting institution;
- The collection of Wi-Fi data by Google Street View cars;
- The collection of geolocation data by TomTom from their clients.

Some situations required enforcement action by the DPA, as was the case with the Borough of Charlois, part of the municipality of Rotterdam, which collected information about ethnicity or race from underage minority groups. The Dutch DPA imposed a conditional fine on Charlois to stop processing this kind of personal data. Charlois filed an appeal at the Court. Another example is the promise of the Netherlands National Rail (NS) and Trans Link Systems – the issuer of the public transport chip cards – for shorter retention periods of students' travel data. This had to be in force at the latest in May 2012. When the implementation term passed without implementing the shorter retention periods, the Dutch DPA imposed a fine on NS in July 2012.

[15] *Veiligheidshuizen* are platforms wherein the police, the public prosecutor and the board for child protection work together in order to prevent recidivism among young offenders.

In addition to conducting investigations, the Dutch DPA advises the government on draft legislation before bills are sent to the parliament. Following the advice from the Dutch DPA, proposals are (sometimes) amended in order to avoid privacy violations. Among others, the Minister of Security and Justice has asked the Dutch DPA to advise on the introduction of a system whereby the lawyers' telephone number would not be recognised and subsequently the conversation could not be tapped. The Dutch DPA welcomed the introduction of such a system to guarantee lawyer-client privilege but advised to include some clarifications and specifications.

Organisation	Dutch Data Protection Authority
Chair and/or College	Jacob Kohnstamm, Chair Madeleine McLaggan, Member of the College; Vice Chair Jannette Beuving, Member of the College (until 1 September 2011) Wilbert Tomesen, Member of the College (as of 1 December 2011)
Budget	Allocated: EUR 7 631 000 Executed: EUR 7 731 000
Staff	80.5 FTE (83 employees)
General Activity	
Decisions, opinions, recommendations	298 (investigations, guidelines, code of conduct, prior checks, sanctions and advice in legislative process).
Notifications	3 939
Prior checks	170
Signals[16] from data subjects	Issues signalled to the DPA through its website: n/a Incoming emails: n/a Incoming telephone calls: n/a Of all these incoming signals, the sectors most issued were Trade and Services (1871), Public Administration (954) and Health and Care (686).
Signals from data subjects –total-	Number of qualified signals dealt with: 5 790
Advice requested by parliament or government	35

[16] Since April 2011 all citizen contacts are registered as a signal. These signals are used to prioritise our tasks. Therefore, signals are not registered by the way they come to hand, but to which sector they are subjected.

Other relevant general activity information	
Inspection activities	
Inspections, investigations	85
Sanction activities	
Sanctions	6
Penalties	N/A
DPOs	
Figures on DPOs	264 DPOs notified to the DPA (on 8 August 2012).

B: Information on case-law

Legitimate interest; proportionality and subsidiarity

The Bureau Krediet Registratie (Bureau of Credit Registration, BKR) registers consumer loans. The BKR maintains databases with the personal data of consumers that contain among others their name, address and scope of their debts and credits. These databases of the BKR are accessible to all its members.

In this case, Mr X had an overdue payment for his loans at the Santander Bank. Even after satisfying this loan, the BKR kept Mr X registered as a debtor. Mr X requested the BKR to remove his personal data, but this was refused.

Mr X went to court to enforce the removal of his personal data from the BKR system. In this case, the Supreme Court of the Netherlands ruled that processing of personal data is only allowed when it is legally defined, explicitly determined and has a legitimate interest. Furthermore, the Supreme Court supplemented to these criteria that even when it is legally allowed to process personal data for a legitimate interest, it should be judged on a case-by-case basis whether it is necessary to process this data in order to achieve legitimate interest. In this case the Supreme Court ruled that there was no legitimate interest anymore to signal Mr X as a debtor now he had paid back his loan. Therefore, the personal data of Mr X should be removed from the database.

The Supreme Court also refers to Article 8 of the European Convention on Human Rights. In this context, the processing of data is only allowed when the interests of the data subject are not disproportionately harmed in regard to the interest pursued (proportionality); and the purpose cannot be achieved in another way (subsidiarity). In this case, the interests of the subject were harmed disproportionately.

POLAND

A. Summary of activities and news

The most important event connected with the activities of the Inspector General for Personal Data Protection (GIODO) was the entry into force as of 7 March 2011 – after almost three years of intensive works – of the amended Act on Personal Data Protection. The provisions that entered into force on 7 March granted to GIODO the powers of an enforcement authority in the scope of administrative enforcement of non-pecuniary obligations (Article 12 point 3), the right to address state authorities, territorial self-government authorities, state and municipal organisational units, as well as other organisational units and natural and legal persons in order to ensure efficient protection of personal data, as well the right to request competent authorities to undertake legislative initiatives and to issue or to amend legal acts in cases relative to personal data protection. The entity receiving the address or request from GIODO shall give an answer in writing to such address or request within 30 days of its receipt. Moreover, preventing or hindering the performance of inspection activities by GIODO's inspectors shall be punishable by a fine and restriction or deprivation of liberty of up to two years.

In 2011 GIODO continued its involvement in the legislative process on the draft Act on exchange of information with law enforcement authorities of Member States of the European Union – being an important legal act from the data protection perspective, and issued opinions on the draft. The Act was passed on 16 September 2011 and entered into force as of 1 January 2012. What is important in the Act on exchange of information with law enforcement authorities of Member States of the European Union it that it introduced changes to the Act on Personal Data Protection. Namely, in Article 43, paragraph 1 of the Act on Personal Data Protection, point 2c was added which provides for exemption from the obligation to notify data filing systems of registration for the controllers of such data which are processed by competent authorities on the basis of the provisions on exchange of information with prosecuting bodies of Member States of the European Union. In Article 26(a), paragraph 1 concerning issuing a decision in an individual case of the data subject based on automated processing of personal data, a new prerequisite legitimising such action was added which is existence of a legal provision which provides for measures to safeguard the data subject's legitimate interests. Modified Article 47 paragraph 1 sets forth that the transfer of personal data to a third country may take place only, if the country of destination ensures an adequate level of personal data protection in its territory. According to the added paragraph 1(a) in this Article the adequacy of the level of personal data protection referred to in paragraph 1 shall be evaluated, taking into account all the circumstances concerning a data transfer operation, in particular the nature of the data, the purpose and duration of the proposed data processing operations, the country of origin and the country of final destination of the data, as well as the legal provisions being in force in a given third country and the security measures and professional rules applied in this country. Paragraph 2 of Article 47 was clarified and states that the provision of paragraph 1 shall not apply if the transfer of personal data results from an obligation imposed on the data controller by legal provisions or by the provisions of any ratified international agreement which guarantees an adequate level of data protection.

Further significant events consisted of appointing a new organisational unit of the GIODO Bureau – the Administrative Execution Team – and specifying the seats and territorial jurisdiction of local offices of the Bureau (under the Regulation by the President of the Republic of Poland of 10 October 2011 as regards granting the statutes to the Bureau of the Inspector General for Personal Data Protection).

Organisation	Bureau of the Inspector General for Personal Data Protection (GIODO)
Chair and/or College	Dr Wojciech Rafał Wiewiórowski, Inspector General for Personal Data Protection
Budget	PLN 14 700 000
Staff	131
General Activity	
Decisions, opinions, recommendations	1 110 decisions issued.
Notifications	11 845 personal data filing systems registered.
Prior checks	As a result of registration procedures (prior checking) 2 298 personal data filing systems containing sensitive data have been entered in the register of personal data filing systems; processing of personal data filing system containing sensitive data can start only after completion of the registration procedure.
Requests from data subjects	3 935 legal questions were sent by email or by post (not only by data subjects, but also by persons interested in the issues related to personal data processing). 2 796 opinions and recommendations were given in total. 4 118 explanations were also provided through GIODO's information hotline.
Complaints from data subjects	Complaints concerned infringement on personal data protection, including: • Public administration (80 complaints); • Courts, public prosecutor's office, the police, bailiffs (32 complaints); • Banks and other financial institutions (94 complaints); • Internet (78 complaints); • Marketing (18 complaints); • Housing related (69 complaints); • Social, property and personal insurance (13 complaints); • Schengen Information System (4 complaints); • Telecommunications (48 complaints);

	• Employment (35 complaints); • Other (178 complaints).
Advice requested by parliament or government	Opinions were expressed on 592 draft acts 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	199 inspections, including 104 sectoral inspections and 95 inspections conducted in connection with complaints submitted against personal data processing and personal data filing systems notified to registration, and as a result of information obtained by GIODO from external entities. Sectoral inspections were conducted in the following sectors: • 21 inspections in public administration; • 10 inspections regarding personal data processing in SIS and VIS in the National Information System; • 15 inspections at companies providing tax and financial advisory services; • 5 inspections at entities providing health care services; • 17 inspections at employment agencies; • 14 inspections at entities organising mass events on stadiums; • 10 inspections at public telecommunications network operators and publicly available telecommunications services providers; • 12 inspections at nursery schools. As result of conducted inspections, 66 administrative proceedings were instituted in order for GIODO to issue administrative decisions ordering to restore the proper legal state.
Sanction activities	
Sanctions	In 2011 GIODO made 10 notifications on suspicion of crime, 4 of which concerned suspicion of crime committed with the use of the Internet. The number of notifications decreased by more than a half compared to 2010 (23 notifications in 2010).

Penalties	
DPOs	
Figures on DPOs	N/A.

B. Information on case-law

In 2011 the judgment by the Supreme Administrative Court of 19 May 2011 was crucial from the perspective of personal data processing in the sector involving Internet activity. The judgment sets forth that in each case where the IP number allows the indirect identification of a given natural person it should be considered as personal data within the meaning of Article 6, paragraphs 1 and 2 of the Act on Personal Data Protection. Another interpretation would be inconsistent with constitutional provisions contained in Articles 30 and 47 of the Constitution of the Republic of Poland. The Court unambiguously stated that IP address (Internet Protocol Address) constitutes personal data.

In the judgment of 24 October 2011 the Voivodeship Administrative Court in Warsaw shared GIODO's view concerning the erasure of personal data from the National Police Information System (KSIP). The Court stated that the provisions of the Act on Personal Data Protection and not the provisions of the Police Act, which entitle the Police to create KSIP, shall be applied to the erasure of personal data stored in KSIP.

C. Other important information

An important element of GIODO's activity is issuing opinions on draft legal acts. Among draft acts submitted for review to GIODO in 2011, draft acts on ICT databases are of special importance. The Polish DPA paid particular attention to various draft acts regulating the functioning of databases such as: educational information systems (SIO), information systems in health care and the Central Register of Entities – National Register of Taxpayers (CRP KEP). Moreover, in connection with the organisation of UEFA EURO 2012, except for the above-mentioned ICT databases, GIODO paid special attention to the draft Act amending the Act on Mass Events Security and certain other acts. GIODO concentrated also on continuing the legislative process on the draft Act on information exchange among EU Member States, as well as on guidelines of the draft Act on reduction of information obligations and reduction of administrative burdens for citizens and entrepreneurs. It also needs to be indicated that GIODO expressed its view on the proposed amendment to the Act on Personal Data Protection. In addition to draft acts – including the ones mentioned above, examples of the most important ones – GIODO issued a series of opinions on draft regulations related to generally understood personal data processing issues.

In the reporting period the increasing trend in the number of registered personal data filings systems as compared to previous years (in 2009: 6 465, in 2010: 9921, in 2011: 11 845) continued. It was possible, inter alia, due to the fact that the declarations did not contain such a quantity of errors, as was the case in previous years. Undoubtedly, this result was influenced by the legislative, educational, organisational and technical activities undertaken by GIODO in 2011 and in previous years that led to significant decrease in the number of issued decisions on refusal of registration (in 2010: 453, in 2011: 105), while the number of registered files increased.

On the occasion of the European Data Protection Day, on 31 January 2011 the Inspector General traditionally organised an Open Day for all citizens at the seat of his Bureau, and conference, Data Retention in a Democratic Legal State. Also, as usual the European Data Protection Day was celebrated in Brussels.

On 21 September 2011 one of the most significant events, i.e. the International Data Protection Conference was organised within the framework of the Polish Presidency in the Council of the EU by the Polish Ministry of the Interior and Administration and the Inspector General for Personal Data Protection in Warsaw. The partners of the Conference were the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information, the Ministry of Public Administration and Justice of Hungary, the Council of Europe, the Academy of European Law and the Spanish Ministry of Justice.

On 15 June 2011 the Workshop for data protection authorities of EU Member States entitled, BCR in practice – DPA sharing experience was organised by the Inspector General for Personal Data Protection at its seat in cooperation with the French Data Protection Authority (CNIL). Its purpose was to exchange experience and knowledge on the practical use of BCRs. Among the issues addressed at the Workshop was, among others, the methodology for analysing of BCR applications.

On 4-5 October 2011, the 23rd Case Handling Workshop was organised by GIODO in Warsaw. The event was attended by representatives of DPAs operating both at the national and regional level, as well as by representatives of the European Data Protection Supervisor. The Workshop was aimed at a practical exchange of experience between employees of particular DPAs dealing with case handling and inspection performance. During the plenary sessions and breakout sessions, among others the following issues were touched upon: cross-border cases handling, personal data protection in connection with the activity of social networking websites and other online services, audit/inspection methodology and privacy in the workplace.

In 2011 GIODO continued publishing information brochures from the ABC of personal data protection series and published the following guides:

- Guide on Personal Data Protection during Election Campaigns;

- Guide on Personal Data Protection in the Orthodox Church, a joint declaration of the Polish leader of the Orthodox Church Metropolitan Sawa and GIODO;

- Guide entitled, Selected data protection issues. Handbook for entrepreneurs, was issued within the framework of the partnership project "Raising awareness of the data protection issues among the entrepreneurs operating in the EU" put into practice jointly by the Bureau of the Inspector General for Personal Data Protection, Czech Office for Personal Data Protection and Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information (in Polish, English, Czech and Hungarian versions).

PORTUGAL

A. Summary of activities and news

The year 2011 was marked by an increase of the DPA's activity, reflected in the numbers of proceedings that reached a record figure.

One of the most important aspects to be highlighted is the launch of the electronic notification system, covering all kinds of notifications, as part of the ongoing process of dematerialisation, enabling the DPA to speed up significantly its internal procedures and to improve its response time, while facilitating a faster and easier way for data controllers to comply with their notification obligations.

It should also be stressed, at institutional level, the good cooperation developed with other national regulators, in order to discuss convergent issues, or with some governmental departments, to closely follow up new projects with data protection implications and also to provide advice on discussions held at European level.

The Portuguese DPA continued raising awareness in data protection, by promoting several initiatives, such as a colloquium organised together with the Direct Marketing Association on data protection and marketing, or the activities for children of Project DADUS with the participation in 20 sessions at schools of 1 500 students, and the promotion of the second edition of the contest "A Slogan for Privacy".

Concerning the inspective activity, the DPA increased the number of on-the-spot inspections and performed an audit to law enforcement authorities and to telecoms providers.

Organisation	
Chair and/or College	Collegiate body composed of 7 members: Filipa Calvão (President), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Barroso, Luís Paiva de Andrade, Vasco Almeida.
Budget	Budget allocated: EUR 3 326 388.13 State budget: EUR 1 308 280.00 DPA own receipts: EUR 2 018 108.13 Budget executed: EUR 1 719 550.60
Staff	23 (Secretary-general: 1; International Relations and Communication Service: 1; Legal Service: 9; Inspection Service: 3; Front Office: 2; Administrative and Financial service: 7.
General Activity	
Decisions, opinions, recommendations	14 913 binding decisions (including 13 307 authorisations for data processing, 75 opinions on draft law and the remaining concerning infractions procedures, complaints, requests of

	access to data by third parties, Schengen Right of Access, and others.
Notifications	16 141
Prior checks	14 852
Requests from data subjects	Figures not available.
Complaints from data subjects	489 (224 related to video surveillance systems and 86 with data processing in the employment context).
Advice requested by parliament or government	72 prior opinions on draft law containing data protection dispositions.
Other relevant general activity information	18 023 new proceedings (notifications, complaints, opinions, infractions, access by third parties). 181 requests concerning the exercise of the right of access and deletion to the Schengen Information System (indirect access through the DPA). 303 requests for opinion from telecom providers concerning the lifting of the confidentiality of the caller in case of disturbing calls.
Inspection activities	
Inspections, investigations	984 investigations started (infraction proceedings), including the performance of 249 inspections on the spot.
Sanction activities	
Sanctions	197 fines applied by the DPA.
Penalties	± EUR 333 000 applied by the DPA.
DPOs	
Figures on DPOs	N/A

B: Information on case-law

No case-law relevant for this report.

C: Other important information

www.cnpd.pt

ROMANIA

A. Summary of activities and news

Organisation	**National Supervisory Authority for Personal Data Processing**
Chair and/or College	Georgeta Basarabescu
Budget	RON 3 320 000 RON (approximately EUR 772 093).
Staff	41, plus the President and the Vice-president of the authority.
General Activity	
Decisions, opinions, recommendations	1 214 (of which, 1 normative decision).
Notifications	11 223
Prior checks	1
Requests from data subjects	90
Complaints from data subjects	404
Advice requested by parliament or government	58
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	214 (on-the-spot).
Sanction Activities	
Sanctions	50 fines to a total amount of RON 61 300 RON (approximately EUR 14 222).
Penalties	41 warnings.
DPOs	
Figures on DPOs	-

B. Information on case-law

Case-law 1

The supervisory authority was notified about two cases concerning the processing of employees' biometrics, in order to monitor their working hours. In order to verify those aspects, certain investigations were carried out with the following outcomes:

- The introduction of electronic systems for checking working hours with info collected, by scanning fingerprints. Hence every employee was obliged to use this biometric device at every entry/exit from the unit, in order to register their effective working hours;

- The introduction of such a decision, taken by the management of public institutions (a hospital and a City Hall) had the intention of imposing on employees observation of the working hours, whereas, previously a presence register was signed, whereby some employees registered delays and absences or signed for other colleagues;

- The workers were notified of the decision to introduce the new time register system shortly before implementing it;

- Only in one of the two cases investigated was the express consent of the employees in this regard requested; however, at the time that the employees were first informed of the system, they were warned that if they refused to accept the use of this biometric timekeeping system, they would not be paid for the hours not recorded in it, resulting in the termination of the employment contract;

- Although the electronic system aimed at giving up the previous system of making this employee signing the presence register, both entities being investigated were allowed, however, for certain individuals or departments, to still use those presence registers;

- The obligation to notify the processing of personal data (biometrics) in order to emphasise the working hours has not been carried out in accordance with the provisions of Law No 677/2001 and of the decision of the president of the supervisory authority No 11/2009 respectively, within 30 days before starting the processing.

Based on those findings, the supervisory authority created the following measures:

- The contravention sanction of the controlled entities, for committing the contraventions provided by Article 31 (failure to comply with the notification obligations), Article 32 (excessive processing of biometric data by reference to the purpose of processing and failure to transmit the response to the complaint received within legal term) and Article 33 (the failure to perform security back-up) of Law No 677/2001;

- The issuance of a suspension decision and following a decision ordering the cessation of the processing of biometric data of employees for working hours registration reasoning.

When issuing the decisions, the supervisory authority took the following into consideration:

The stated purpose of the data processing, namely, recording the working hours of the employees, could have been achieved by other, less intrusive methods such as utilising the presence register, or using other functions of the electronic system implemented. It was ascertained that the presence of some employees was still being recorded by the use of the presence register. The use of different means to achieve the same purpose had the potential of appearing discriminatory in the application of the internal rules to the employees of the same entity. Moreover, in the context of the employer-employee

relationship, the written consent of the employees in one of these cases could not be assumed to have been freely expressed and informed such as to make the processing legitimate, especially taking into consideration the consequences of refusing to accept the system.

As such, according to Article 4 (1) (c) of Law No 677/2001, as modified and amended, the processing of biometric data of employees was excessive by reference to the purpose for which they were collected and later processed. Following the investigations, the two entities complied with the decisions of the supervisory authority ordering them to cease processing the biometric data of the employees to record working hours.

Case-law 2

Another situation brought to the attention of the supervisory authority related to the processing of personal data from an identity card for the purpose of buying and recharging pre-paid cards. In the absence of any legal basis, the refusal to present an identity card would deprive the consumer/individual of access to a mobile phone service.

Following the investigations carried out, the data controllers were advised to modify the method of providing pre-paid cards, namely, that a copy of an identity card when buying a pre-paid card could only be produced with the written consent of the data subject. As regards recharging the pre-paid card, the supervisory authority ruled that this service should not be conditional on presenting an identity card.

Case-law 3

The supervisory authority received information from students concerning the fact that on the websites of the universities they attended there were profiles where every student had a personal account. Access to the profile page, which contained the personal data of a student and his/her parents (first and last name, the last name after marriage, date of birth, place of birth, sex, religion, series of the identity card, personal identification number, civil and military status, as well as other information regarding the school) was by personal identification number .

Following verification, it was ascertained that this type of profile formed part of an application (University Management System – UMS) designed for institutions of higher education and, from a technical point of view, the authentication was done by means of the personal identification number and the date of birth.

The purpose of processing within this application was said to be to maintain centralised records of all the students, as well as of their school and financial situation, data which were requested by the Ministry of Education, Research, Youth and Sport in order to achieve the unique register at national level.

In these cases, the recommendation of the supervisory authority was to find a unique identification code, other than the personal identification number, as the means for accessing the student profiles.

SLOVAKIA

A. Summary of activities and news

During 2011 the Office for Personal Data Protection of the Slovak Republic (hereafter referred as to the Office) continued to inform the general public via the media, regarding new elements of data protection developments in various areas. The employees of the Office produced television announcements both on the occasion of the Data Protection Day, as well as on specific topics, e.g. child online protection. The Office's experts also met a delegation of the Serbian Information and Data Protection Commissioner whereby they provided lectures on chosen topics.

In addition to this, the Office initiated an important amendment of the Act on Payment Services which foresees informing data subjects that, whenever they pay with a credit card an amount which exceeds a fixed level, their national ID number might be processed. This agreement was concluded after several rounds of negotiations with the Slovak association of banks. Both parties agreed the text of an informative sticker which would be fixed to the sales spots.

Furthermore, the Office was confronted with a cut in its budget in the amount of 10%, which was effectuated under the pretext of the overall reduction in the expenditures of the public administration bodies.

This situation adversely affected the national supervision of the protection of personal data and the execution of the Office's tasks, and even led to laying off employees. Subsequently, on the Office's initiative, the adverse financial situation was examined by the European Commission in the context of a possible infringement procedure. The procedures remained in the initial (pilot) phase for the remainder of 2011.

Organisation	Office for Personal Data Protection of the Slovak Republic
Chair	Mr Gyula Veszelei
Budget	EUR 684 349
Staff	34 in the first half of 2011; 29 by 31.12.2011
General Activity	
Opinions, recommendations	714 + 24 based on the Public Access to Information Act
Notifications	33; as well as notification of PDPOs (personal data protection officials) – 881.
Prior checks	8 (special notifications).
Requests from citizens	714+24
Complaints from citizens	176; 6 repeated complaints.

Complaints from other subjects	33
Advice requested by parliament or government	77
Other relevant general activity information	Inspection proceedings total – 266 Examination of complaints total – 290 Orders binding for individual controllers – 102 Decisions of the president upon objections against Office decisions (Appeals) – 12 Cross-border data flows – 20 decisions upon approval of the international transfers to third countries not ensuring an adequate level of data protection. Criminal Filings – 6
Inspection activities	
Inspections	125 based upon the complaints. 57 *Ex officio* inspections. 36 submissions for explanations. Key topics and issues: • National census: insufficient information to citizens about the anonymity of the personal data acquired in the census; • Loyalty cards: wrong legal basis; illegal combination of personal data processed for purposes other than those for which it was collected; • Video surveillance: inappropriate marking of the monitored area; non-erasure of records within the prescribed time period; illegal provision of records to mass media; unsatisfactory information from persons with access to the camera systems; • Schengen Information system: implementation of the obligation stemming from the national Schengen action plan; inspection of the issuing of Schengen visas in the consular department of the embassy of the SR in Vienna, Austria; inspection in the national SIRENE Bureau, Ministry of Interior of the SR as regards the thorough application of Articles 95, 96 and 99 of the Schengen Convention.
Sanction activities	

Sanctions	9
Penalties	EUR 34 300; Until the end of 2011, the amount of EUR 16.600 has been paid; the rest was ceded to execution proceedings.

B. Information on the case-law

In 2011, there were no court decisions passed as regards appeals against the Office's decisions.. The Bratislava district court heard an action instituted by a joint stock company seeking damages for loss caused by an allegedly illegal decision of the Office. The proceedings were initiated in 2008; however, the Office was not notified of the action and admitted as a co-defendant with the Slovak Republic, represented by the Ministry of Justice of the SR, until 14 July 2011. The court did not arrive at a decision during 2011.

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 2011 the Commissioner initiated 682 cases regarding a suspected breach of the PDPA provisions, 246 in the public sector and 436 in the private sector. In both sectors the most common suspected breaches are of similar nature, involving unauthorised disclosure of personal data by transfer of data to third persons or by unlawful publication of data, unlawful collection of data, inappropriate security of data, in the private sector also unlawful use of data for the purpose of direct marketing and unlawful video surveillance. The Commissioner initiated 136 offence procedures. The number of inspection procedures increased from the previous year.

In addition to the inspection and offence authority competencies the Commissioner issues non-binding opinions and clarifications on specific issues regarding data protection raised by the individuals, data controllers, public bodies and international bodies. In 2011 the Commissioner issued 2 143 opinions and clarifications, which shows a significant increase from the previous year (1 859) and may be attributed to the transparent work and intensive public campaigning of the Commissioner. The Commissioner is, under the PDPA, also competent 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.

In the course of its awareness raising activities, the Commissioner continued its preventative 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 expanded the scope of its tools for awareness raising and introduced a new format for the special reports: the first covered loyalty cards. It also issued *Guidelines on Tools for Online Privacy Protection*. In the context of the European Data Protection Day the Commissioner organised an event intended to draw attention to the importance of personal data protection in the modern ICT society, with the premiere of a documentary film "Erasing David". On this occasion the Commissioner awarded three data controllers for good practice in personal data protection – one of the awards being dedicated to the efforts in respect of 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 is first 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 on safer and user friendly e-identities, and on the strategy of the information society development in the period between 2011 and 2015. The Commissioner was consulted by the legislator and competent authorities regarding 27 acts and other legal texts in the fields of underage delinquents, real estate records, road tolling, electronic commerce and electronic signatures, higher education, children with special needs, parliamentary elections, tax and criminal procedures and the penal code, etc.

The Commissioner actively participated in a number of international bodies: The Article 29 Working Party, Joint Supervisory Body of Europol, Joint Supervisory Authority for Schengen, Joint Supervisory Authority for customs, EURODAC, WPPJ, International Working Group on Data Protection in Telecommunications, Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to the 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 1 468 000
Staff	30 employees: the cabinet (6 – 2 of the employees are also supervisors, and 2 are legal advisers) administrative (3), access to public information legal advisors (10), data protection researchers and advisors (4), data protection supervisors (11).
General Activity	Data protection and access to public information.
Decisions, opinions, recommendations	261 opinions and recommendations based on requests from data subjects or data controllers.
Notifications	Approximately 200 notifications on personal data filing systems.
Prior checks	25 prior checks: 8 on biometrics, 4 on the transfer of data to third countries, 6 on connection of filing systems.
Requests from data subjects	2 143 requests for opinions/clarifications from data subjects.
Complaints from data subjects	617 complaints from data subjects in total, 444 complaints qualified. Areas: 218 unlawful transfer or disclosure of data, 128 unlawful collection of data, 79 direct marketing, 89 video surveillance, 43 data security, 60 other. Additionally 85 complaints regarding data subject rights were handled.
Advice requested by parliament or government	The legislator and competent authorities drafting the legislation consulted the Commissioner regarding 27 acts and other legal texts, among other Healthcare Databases Act, Treatment of Juvenile Offenders Act, Toll Collection Act, Real Estate Records Act, Criminal Procedure Act, etc.
Other relevant general activity information	The Commissioner in 2011: • Continued its preventative work (lectures, conferences) together with the Centre for Safer Internet of Slovenia; • Participated in inter-departmental work groups on e-government projects, among others on e-identity; • Published Guidelines on tools for data protection online, and a Special report on loyalty cards; • Was consulted regarding a number of acts; • Continued strong international involvement and participation.
Inspection activities	
Inspections, investigations	682 inspections: 246 in the public sector, 436 in the private sector.

Sanction activities	
Sanctions	136 offence procedures initiated (43 in the public sector, 66 in the private sector, 27 private persons), of these 30 warnings, 52 admonitions, 12 fines and 7 payment orders issued.
Penalties	The DPA imposed EUR 50 035 in penalties, administrative taxes excluded.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

The Information Commissioner received numerous complaints regarding **veterinary offices** sending dog owners notifications on vaccinations and at the same time offering them other services. It was found that the veterinary offices had obtained dog owners' personal data from the central register of dogs, which does not have the status of a public register, and where data may be used only for legally determined purposes (maintaining the register of dogs and dog owners, control over regular vaccinations and monitoring of bites, as well as for statistical purposes). Veterinary offices should not have used such data for direct marketing despite having access to it. For the purposes of direct marketing only the personal data of the dog owners who are customers of a certain office may be used, as well as data from publicly accessible sources. The Information Commissioner issued the veterinary office a sanction.

The Information Commissioner considered a case involving the direct **marketing of geodetic services** offered to individuals whose buildings were not entered in the register at the portal Prostor (English: Space). Although the information was obtained from publicly accessible sources, the data controller violated PDPA provisions due to the fact that only the following information may be used for the purpose of direct marketing: the name of the person, and his/her permanent or temporary address, phone number and fax number. In order to use the information that an owner has not yet entered his property in the register the data controller would need explicit consent.

The Commissioner received a complaint about an **online dating site**'s users' names, email addresses and passwords being disclosed online. It has been established that the operator of the website entrusted the design of the website to an Indian contractor. The product did not include measures for traceability of the data processing, and poor programming enabled the perpetrator to gain data on 7 000 site users. The website operator was also found in breach of the provisions on contractual data processing, because it did not conclude a contract with the data processor. A data transfer to third countries without legal basis was additionally established. The Commissioner ordered the website operator to stop the processing of data and to notify all the users of the forum of the incident.

The Information Commissioner discovered that on the website of the **National Electoral Commission** personal data were published: of the candidates in the past parliamentary elections, as well as of candidates for past local elections. Sectoral law regulates the publication of candidates' personal data only with regard to the period before an election but not with regard to the period following it. The Commissioner held that the candidates' personal data are published for the purpose of voters being able to make an informed and free decision as to which list and candidate they would vote for. Since the purpose of personal data processing had already been fulfilled for the past elections, the data controller should have deleted the candidates' data.

The Commissioner handled a case where **spatial photography containing images with identifiable individuals** was published on the website of a professional photographer. In the procedure spatial photography was considered in the context of the purpose of publication and identifiability of the individuals in the images. The Commissioner held that the purpose of the depiction of natural and cultural heritage can be achieved also without depiction of identifiable passers-by. The interest of the photographer in the publication in that case doesn't override the interest of the passer-by to decide freely whether he/she wishes to be identifiable in the image. That is why such images have to be rendered anonymous before publication on the Internet, so that the individuals are no longer identifiable. In its related opinion the Commissioner also pointed to the difference between street photography and spatial photography.

C. Other important information

In terms of **international cooperation** the Commissioner was also active in the field of bilateral international cooperation. In 2011, it hosted representatives from a number of countries, such as Croatia, Serbia, Kosovo, Montenegro and Macedonia. As a Junior Partner it continued with the implementation of the twinning project IPA 2009, No MN/09/IB/JH/03 – Implementation of Personal Data Protection Strategy in Montenegro – to which it was selected in 2010, together with the project leader, the Ludwig Boltzmann Institute for Human Rights from Austria. In November 2011 the Information Commissioner was selected by the European Commission to implement the Twinning Light Project SR/2009/IB/JH/01, Improvement of Personal Data Protection, which is focused on improving personal data protection in Serbia. The Information Commissioner also carried out an inspection at the embassies of the Republic of Slovenia in Pristina and Cairo, where it reviewed, among other issues, the lawfulness of personal data processing in procedures for obtaining a Schengen Area visa and within the Visa Information System (VIS).

In terms of **policy issues** that the Commissioner has dealt with extensively, it is necessary to mention the increasing use of video surveillance, in spaces like saunas, changing rooms, children's playgrounds, and in some other public areas such as walking paths. The Commissioner also notes an increase in cases related to online marketing and unsolicited emails, where the senders often cannot demonstrate they have obtained the consent of the recipients, do not respect opt-outs and do not inform the recipients of their rights. Regarding the security of data processing the Commissioner notes that security is often not comprehensive enough to satisfy the conditions set by the PDPA. In a number of cases personal data were found to be accessible on the Internet.

Furthermore, the Information Commissioner noted that numerous data controllers face the dilemma of whether to use **cloud computing**, which raises certain issues regarding its consistency with legislation in the field of the protection of personal data and privacy. Organisations that decide to use cloud computing often do not possess enough information on where their personal data will be located and how it will be protected, however, without such information it is difficult to carry out appropriate risk analyses prior to making a decision to use the cloud. The Information Commissioner issued a few opinions regarding cloud computing and at the end of 2011 it also began to prepare guidelines intended to help data controllers in the process of deciding to use this product.

SPAIN

A. Summary of activities and news:

Information to citizens and protection of their rights

The activity of the AEPD directly related to providing information and protection to citizens has significantly increased in 2011. The number of requests for information to the citizens' helpline has grown 30% (with nearly 135 000 requests) and the website has received a total of three million visits. In the same line, the number of claims[17] grew 35% in 2011, reaching a total of 2 230 requests. More than 60 % of the decisions made by the AEPD in response to these requests dealt with the rights to erasure or to object. This trend is also followed by claims on the "right to be forgotten", with figures that have evolved since three claims in 2007 to 160 in 2011. Additionally, the number of complaints[18] was 50% higher than in 2010, with nearly 5 500 complaints.

The protection of children is a priority for the AEPD. In 2011 all existing DPAs in Spain (AEPD and sub-state agencies of Catalonia, Madrid and the Basque Country) made available a training tool called "Register, enter, unsubscribe. Protect your rights and control your data". The tool is an adaptation to the Spanish environment of the original materials devised by the Irish Data Protection Commissioner. This educational resource will be followed by a more comprehensive tool which will be launched in 2013.

Facilitate implementation of the law

Data controllers may ask for clarification of the relevant provisions of the Data Protection law in especially complex cases. The AEPD issued nearly 500 legal reports in 2011. The AEPD has also issued more than 100 reports on draft legislative and regulatory measures. The reports are mandatory for the Government and although not legally binding, they are influential in the legislative process.

In April 2011, the AEPD started a new information system (RENO) developed to improve the efficiency of operations associated to notification, file registration and authorisation of international transfers. The application includes individual electronic signature and electronic seal systems to facilitate the issuance and notification of resolutions, among others.

Legal changes

In March, the Spanish Data Protection Act (LOPD) was amended by Law 2/2011 on Sustainable Economy. The amendments have affected the sanctions system in a number of ways. On the one hand, the classification of infringements has been modified. The categories (not serious, serious and very serious) remain the same, but the activities included in each category have been adjusted. The minimum and maximum amounts of possible fines for each type of infringement have been also slightly modified. It is particularly relevant that the amended provisions set objective criteria for modulation of sanctions, provide for the possibility of reduction of sanctions if preventative/proactive measures are in place and

[17] Requests for a decision of the Agency in order to uphold the data protection rights of the claimant in cases of non-compliance of a specific controller

[18] Requests for a decision of the Agency declaring the existence of an infringement of the law, ordering the end of that infringing activity and imposing a sanction.

introduce a "preventative warning" that may replace fines in specific cases (first infringement which is not "very serious" if other conditions are met).

International cooperation

In June 2009 the AEPD was awarded the lead in a Twinning project to be developed in Croatia. The Project sets a framework of cooperation between the Spanish and Croatian DPAs in order to prepare Croatia's access to the EU. During 2011 the AEPD and the Croatian Agency have jointly carried on the activities covered by the Project, due to finish in 2012.

Organisation	Spanish Data Protection Agency
Chair and/or College	Mr José Luis Rodríguez
Budget	EUR 14 437 970.00
Staff	156 (154 civil servants – 2 public employees) and 1 Commissioner.
General Activity	
Decisions, opinions, recommendations	Number of decisions related to citizen claims: 7 233; Legal reports: 140
Notifications	638 533 notifications related to public and private files. Total of Notified files at the end of 2011: 2 609 471
Prior checks	N/A
Requests from data subjects	134 635 requests to the Helpline (in writing, by phone, by web and through the front desk). 484 requests of the report addressed to the Legal Department (246 from public administrations and 238 from individuals or private entities).
Complaints from data subjects	5 389 complaints lodged by data subjects. Sectors such as telecommunications and video surveillance presented substantial increases (17.78% and 6.35% respectively) as well as other relevant fields like Internet and commercial advertising.
Advice requested by parliament or government	The AEPD issued legal opinions on a total of 110 general draft legal texts or amendments of existing legal texts, including the Transparency Law, Supervision of Private Insurance Law, the General Telecommunications Law and the Anti-Doping Law.
Other relevant general activity information	2 892 516 acts of accessing via the web (7 923 daily average). 3 500 883 online consultations to the Public Register. 175 authorisations for International Transfers were approved by the

	Director.
Inspection activities	
Inspections, investigations	5 389 previous investigations and 2 230 procedures for the protection of rights. 7 233 Resolutions from inspection procedures divided into 1 939 related to protection of rights claims (access, rectification, erasure and objection) and 5 294 procedures related to the sanctioning power. The inspection department also carried out *ex officio* investigations in different areas: - Cloud computing; - Transfer of business data – Inspections on the sale of debt by telecommunications operators and financial institutions (ongoing); - European Arrest Warrants in Spain; - Analysis of contractual clauses of the Telecomm operators.
Sanction activities	
Sanctions	Out of 898 sanctioning resolutions, 96.46% were related to the Data Protection Act; 3.02% were based on the Act on Internet society services (spam) and just 0.52 % under the General Act on Telecommunications' (advertising by fax).
Penalties	EUR 19 597 905.97 (+12% with regard to 2010).
DPOs	N/A
Figures on DPOs	N/A

B. Information on case-law

The "preventative warning" introduced by the amendment of the Data Protection Law has been extensively used in 2011. Nearly 40% of all decisions declaring the existence of an infringement were closed with a warning instead of a fine. Cases where the "preventive warning" has been applied typically include unintentional mistakes, infringements by private individuals due to insufficient knowledge of the DP law and infringements which involve breaches of provisions on formal or administrative requirements. Elements such as the degree of cooperation of the controller in addressing the breach, the sensibility of the affected data, the economic impact of the infringement or the relationship of the data processing operations with the main activity of the controller are regularly taken into account in deciding whether to issue a warning or to impose a fine.

Case-law National Court:

In 2011 several judgements that decided on the balance between the right to data protection and other fundamental rights and freedoms were especially relevant.

- With regard to the right to information, a judgement of the National Court of 29 September declared compliant with the LOPD the publication in the media of photographs of a victim of the terrorists attacks of March 2004 in Madrid, considering that such pictures are relevant in relation to the information that the media intended to offer.

- The right to freedom of a trade union association was considered to prevail over data protection rights in cases where information is made public that is relevant for the workers and publication is limited to the workplace itself.

Case-law Supreme Court

On November 24 a judgement of the Court of Justice of the EU declared that Article 7(f) of Directive 45/96 cannot be interpreted in the way the LOPD (*Ley Orgánica* 15/1999, *de Protección de Datos*) does. This judgement solves a question posed by the Spanish Supreme Court in the context of an appeal in which some companies challenged several articles of the administrative regulation that implements the Article of the LOPD that transposes Article 7(f) of the Directive. Although the case concerned the administrative regulation, the Supreme Court also asked the European Court whether the Article of the Law in which the regulation is based is compatible with the European Directive. The European Court's judgement considers that Article 7(f) has direct effect and therefore makes the corresponding Article of the Spanish Data Protection Law inapplicable. Additionally, the Spanish Supreme Court has declared null and void some of the contested Regulation provisions.

SWEDEN

A. Summary of activities and news:

Supervision

E-government

The Data Inspection Board has published a specific information leaflet on personal data processing and e-government. In addition to this, we have published information on our website regarding privacy by design that is relevant in this context. We have also given opinions on proposed legislation in this matter and carried out a specific audit project regarding the electronic exchange of information between authorities. Other audits in the e-government area have been directed towards health and medical care and social service.

Cloud computing

In order to clarify the demands that the Personal Data Act lays down in terms of cloud computing, the Data Inspection Board audited a number of local government authorities and companies who use such services. The project resulted in an information leaflet with a checklist of the data protection requirements in cloud computing services.

Camera surveillance

A massive audit project was concluded that regarded camera surveillance in the workplace, apartment buildings and schools. This resulted in information leaflets with checklists of the considerations that need to be made in relation to camera surveillance.

Awareness raising

Making people aware of data protection and privacy issues is an important part of our strategy – we have continued to work proactively and to make privacy and data protection issues visible. In 2011, the number of visits on our website increased by 24%. The Data Inspection Board also noted a significant increase in the number of questions to our data protection helpdesk. Furthermore, for the fourth year, the Board published a pamphlet called the Privacy year (2011) which compiles and summarises the legislation, legislative proposals, decisions and other items that have had privacy implications during the year.

Other activities

One representative of the Data Inspection Board was the rapporteur of the Article 29 WP's sub-group on Health Data, regarding the drafting of a working document about epSOS (European Patients Smart Open Services), WP 189.

In view of the entry into force of the new Police Data Act in March 2012, more focus was also made on data protection matters in the law enforcement area.

Organisation	
Chair and/or College	Göran Gräslund Director-General
Budget	SEK 37 million = EUR 4.2 million
Staff	47
General Activity	
Decisions, opinions, recommendations	247 audits were initiated in 2011. 107 opinions on legislative proposals. 61 opinions in consultation with data protection officials. 13 guidelines, recommendations and reports.
Notifications	215
Prior checks	238
Requests from data subjects	206 formal requests. Informal questions by phone and email to our helpdesk: 4 700 (email) 7 500 (phone).
Complaints from data subjects	312
Advice requested by parliament or government	107 opinions on legislative proposals.
Other relevant general activity information	Lectures, seminars and conferences: 42 Press releases: 67
Inspection activities	
Inspections, investigations	43 field audits. 134 desk audits. 70 audits by questionnaire. Key topics: cloud computing, camera surveillance, GPS positioning systems of employees, background checks by recruitment agencies, e-government.
Sanction activities	
Sanctions	None according to the Personal Data Act.
Penalties	Not applicable.

DPOs	
Figures on DPOs	The total number of notified DPOs in 2011 was 6 621. The Data Inspection Board received 61 formal consultations from DPOs and held 9 lectures specifically addressed to DPOs.

B. Information on case-law

The Supreme Administrative Court confirmed the Data Inspection Board's previous decision not to allow camera surveillance in entrance-halls of apartment buildings. The Data Inspection Board had ordered a housing company to stop using camera surveillance in the entrance-halls of their apartment buildings since this made it possible for the company to monitor and map the tenants' habits and acquaintances. The Board's decision was appealed against to the Administrative Court and to the Administrative Court of Appeal who both confirmed the Board's decision. In December 2011, the Supreme Administrative Court confirmed this decision. In a balance of interests, the Court found that there had not been evidence that the buildings were particularly exposed to crime, nor had it been proven that there was any other substantial need for the surveillance. Therefore, the surveillance should be regarded as a privacy infringement and was not in compliance with the Personal Data Act.

UNITED KINGDOM

A. Summary of activities and news:

Public policy developments

The ICO was influential during the passage of the Protection of Freedoms Act providing evidence to the Parliamentary Public Bill Committee. The new Act strengthens privacy in areas such as video surveillance and biometrics, delivers improved transparency and provides even greater guarantees of independence for the ICO. We were also one of the early witnesses to the Leveson Inquiry into the culture, practices and ethics of the press, giving evidence on our reports that first highlighted the unlawful trade in personal information and pressing for the introduction of custodial sentences.

Getting stronger and more tech savvy

We were given new powers enabling the ICO to impose monetary penalties of up to GBP 500 000 for serious breaches of the Privacy and Electronic Communications Regulations. This brings parity to the similar powers that we have been using to increase the effect for serious breaches of the DPA 1998. We continue to press for more powers and submitted a business case to the Ministry of Justice to extend our assessment notice powers to audits in the NHS and local government sector.

Given the importance of technology and data protection the ICO strengthened its office with the appointment of a technology adviser to play a leading role in the Information Commissioner's work on policy development, investigations and complaints handling.

Guidance

We kicked off 2011 by marking European Data Protection Day by launching a new "Personal information toolkit" to help UK organisations handle subject access requests better.

We also issued new guidance on Wi-Fi security settings as a survey showed that 40% of home users do not understand how to secure these. We re-issued data protection guidance to political parties and candidates campaigning for the UK referendum and local and national elections; and issued reminders to the health service to keep patients' personal information secure following enforcement action taken against five health organisations in breach of the Data Protection Act. We also issued guidance to students about their data protection rights to access information about their exam marks.

We provided detailed guidance to those UK websites operators in response to changes in EU legislation requiring them to obtain consent to store or access information on consumers' computers.

We continued to stimulate debate on data protection by hoisting data-sharing events in Cardiff, Belfast and Glasgow for organisations from across public, charity and voluntary sectors to discuss the importance of effective data sharing. We hosted a seminar on data anonymisation in London, with over 100 delegates including experts from a range of sectors. We also held a conference with 100+ delegates in Northern Ireland to discuss a business case for data protection.

Education, education, education

Ensuring that individuals are aware of their information rights is essential and incorporating these into the UK's education systems is vital. We launched a research project to explore ways of doing this in practice. We also teamed up with students at 15 universities across the UK, aimed at raising young people's awareness of information rights and promoting the ICO's work on campus.

Organisation	
Chair and/or College	Mr Christopher Graham (Commissioner)
Budget	GBP 19 695 000 (Notification fee GBP 15 600 000 and FOI grant in aid GBP 4 500 000.
Staff	Total: 378 First Contact – 72 Customer resolution – 102 Enforcement – 34 Strategic Liaison – 18 Policy delivery – 11 Notification – 20 Audit – 32 Administration – 10 Internal governance – 14 Legal – 6 Corporate affair – 22 Facilities 4 Finance 7 IT – 9 Learning and development – 3 Regional offices – 10
General Activity	
Decisions, opinions, recommendations	Personal information toolkit. Freedom of Information guidance. Consulting on anonymisation code of practice.

Notifications	Total data controllers notified 355 292
Prior checks	N/A
Requests from data subjects	Calls on helpline: 217 183
Complaints from data subjects	Number of complaints received for data protection: 12 985 Number of complaints received for freedom of information: 4 633 Number of complaints received for privacy and electronic communications act: 7 095
Advice requested by parliament or government	Responded to 17 consultations.
Other relevant general activity information	Number of "relevant number to be chosen by DPAs". Any relevant figures reflecting the activity of the DPA, for instance number of BCRs approved as a lead DPA.
Inspection activities	
Inspections, investigations	42 audits.
Sanction activities	
Sanctions	2 enforcement notices. 8 search warrants issued. 76 undertakings. 15 prosecutions (1 case resulted in confiscated funds totalling GBP 73 000 to be repaid).
Penalties	We issued 10 civil monetary penalty notices totalling GBP 1 171 000
DPOs	
Figures on DPOs	N/A

All figures given above are from the financial year 2011-2012

B. Information on case-law

Anonymised information and personal data

In February 2005, the ProLife Alliance made a request to the Department of Health, under the Freedom of Information Act 2000 (FIOA), for detailed statistical information about abortions carried in the year

2003. The Department of Health refused the request for the 2003 abortion statistics relying on a number of the FOIA exemptions from disclosure, including the exemption in Section 40 concerning personal data.

Following a complaint to the Information Commissioner about the non-disclosure and an appeal to the Information Tribunal, the matter was heard in the High Court before Mr Justice Cranston in *R (on the application of the Department of Health) v Information Commissioner [2011] EWHC 1430 (Admin)*. The key consideration was whether the detailed abortion statistics were personal data for the purposes of the Data Protection Act 1998 (DPA).

The definition of personal data in the DPA was given detailed consideration as was Recital 26 of the Directive which provides, in part, that "the principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable". The court also considered the Article 29 Working Party Opinion (4/2007) on the concept of personal data and noted that the Opinion had concluded that anonymous data for the purposes of the Directive, could be defined "as any information relating to a natural person, where the person could not be identified, whether by the data controller or by any other person, taking into account all means likely reasonably to be used to identify that individual".

Mr Justice Cranston, following the reasoning of Lord Hope in the Supreme Court in the case of the *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, held that, the fact that the data controller has access to all the information from which the statistical information is derived, does not disable it from processing the data in such a way, consistent with Recital 26 of the Directive, that it becomes data from which a living individual can no longer be identified. If converting the underlying information into statistics can achieve this, the way will then be open for the data controller to disclose the information in statistical form because it will no longer be personal data. Mr Justice Cranston held that the disclosure by the Department of Health of the detailed abortion statistics would not amount to the disclosure of personal data. This judgment provides helpful clarification regarding the inter-relationship between personal data and information that has been rendered anonymous as referred to in Recital 26 of the Directive.

Chapter Three

European Union and Community Activities

3.1. EUROPEAN COMMISSION

EU Data Protection Day 2011, 28/1/2011

The protection of personal data is a fundamental right within the EU. The Commission and the Member States of the Council of Europe celebrated Data Protection Day for the fifth time on 28 January 2011.

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.

To mark Data Protection Day 2011, events were organised not only in Europe, but all over the world to raise awareness about data protection and also inform citizens of their rights and good practices, thereby enabling them to exercise these rights more effectively.

This special day presents an opportunity for individuals to become more aware of personal data protection and what their rights and responsibilities are in this respect.

The major event of Data Protection Day 2011 was a joint high-level meeting on data protection – Data protection (30 years later) – from European to international standards.

As well as addresses by the Secretary General of the Council of Europe, a Vice-President of the Commission and the Director-General of the DG Justice of the Commission, a panel on New European Rules on Data Protection included the Chair of the Consultative Committee of Convention 108, the Council of Europe, the European Data Protection Supervisor and the Chairman of the Article 29 Working Party.

Consultation on the Commission's comprehensive approach to personal data protection in the European Union 15th January 2011

To obtain views on the Commission's ideas – as highlighted in its Communication attached to this consultation – on how to address the new challenges for personal data protection (e.g. fast-developing technologies, globalisation) in order to ensure an effective and comprehensive protection to individual's personal data within the EU.

The Commission received 305 responses to the public consultation: 54 from Citizens, 31 from Public Authorities, 220 from private organisations.

Special Eurobarometer Study – Attitudes on Data Protection and Electronic Identity in the European Union, June 2011

The Special Eurobarometer Study was the largest survey ever conducted regarding citizens' behaviour and attitudes concerning identity management, data protection and privacy, and represents the attitudes and behaviour of Europeans on this subject.

The main findings of the survey were as follows:

- 74% of the Europeans see *disclosing personal information* as an increasing part of modern life.

- Information considered as personal is, above all, financial information (75%), medical information (74%) and national identity numbers or cards and passports (73%).

- Social networking and sharing sites users are more likely to disclose their name (79%), photo (51%) and nationality (47%). Online shoppers' *actual online disclosure of personal information* mainly involves their names (90%), home addresses (89%) and mobile numbers (46%).

- The most important reason for disclosure is to access an online service, for both social networking and sharing site users (61%) and online shoppers (79%).

- 43% of Internet users say they have been asked for more personal information than necessary when they proposed to obtain access to or use an online service.

- The majority of Europeans is concerned about the recording of their behaviour via payment cards (54% vs 38%), mobile phones (49% vs 43%) or mobile Internet (40% vs 35%).

- Almost six in ten Internet users usually read privacy statements (58%) and the majority of those who read them adapt their behaviour on the Internet (70%).

- Over half of Internet users are informed about the data collection conditions and the further use of their data when joining a social networking site or registering for a service online (54%).

- Only one third of Europeans are aware of the existence of a national public authority responsible for protecting their rights regarding their personal data (33%).

- Just over a quarter of social network users (26%) and even fewer online shoppers (18%) feel in *complete* control.

- Europeans use the following types of credentials: mostly credit cards and bank cards (74%), national identity cards or residence permits (68%), government entitlement cards (65%), or driving licences (63%). 34% of respondents have an account they use on the Internet, such as email, or for social networking or commercial services.

- To protect their identity in daily life, 62% of the Europeans give the minimum required information.

- To protect their identity on the Internet, the most usual strategies are technical or *procedural*, like tools and strategies to limit unwanted emails such as spam (42%), checking that the transaction is protected or the site has a safety logo or label (40%), and using anti-spy software (39%).

- Authorities and institutions – including the European Commission and the European Parliament (55%) – are trusted more than commercial companies.

- Less than one third trust phone companies, mobile phone companies and Internet service providers (32%); and just over one fifth trust Internet companies such as search engines, social networking sites and email services (22%).

- 70% of Europeans are concerned that their personal data held by companies and may be used for a purpose other than that for which it was collected.

- 28% are prepared to pay for access to their personal information stored by public or private entities.

- As regards the "right to be forgotten", a clear majority of Europeans (75%) want to delete personal information on a website whenever they decide to do so.

- Even though a majority of European Internet users feels personally responsible for the safe handling of their personal data, almost all Europeans are in favour of equal protection rights across the EU (90%).

- More than four in ten Europeans would prefer the European level of administration for enforcing regulations (44%), while a somewhat smaller number would prefer the national level (40%).

- When asked what type of regulation should be introduced to prevent companies from using people's personal data without their knowledge, most Europeans thought that such companies should be fined (51%), banned from using such data in the future (40%) or compelled to compensate the victims (39%).

- The majority believe that their personal data would be better protected in large companies if these companies were obliged to have a Data Protection Officer (88%).

- Europeans' opinions are divided with respect to the circumstances under which the police should have access to personal data. In contrast, they almost all agree that minors should be protected from (95%) and warned against the disclosure of personal data (96%); and a vast majority are in favour of the special protection of genetic data (88%).

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)

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.

Judgment of the Civil Service Tribunal (First Chamber) of 28 June 2011 – AS v European Commission (Case F-55/10)

Medical secrecy covers, inter alia, information coming to the attention of a health professional in the exercise of his functions, and communicated to him by the person he treats. The right to the protection of medical confidentiality, which is one aspect of the right to respect for privacy, is a fundamental right protected by the law of the Union. These two rights may include restrictions provided that they genuinely meet objectives of general interest pursued by the Union, and do not constitute, in relation to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of the rights guaranteed.

In this regard, and with reference to Article 8 of the European Convention on Human Rights, interference by a public authority with the right to respect for private life, which includes the right to keep one's state of health secret, may be justified provided it is "prescribed by law", pursues one of the objectives set out in paragraph 2 of this article, such as "economic well-being" and "protection of health", and is necessary "to achieve these goals".

This is not the case of the use by an institution, in the context of an action brought by an official, of elements contained in the medical record of the individual for the sole purpose of developing an argument that would demonstrate his lack of interest in acting.

Judgment of the Civil Service Tribunal (First Chamber) of 5 July 2011 – V. v European Parliament (Case F-46/09)

The right to respect for private life guaranteed by Article 8 of the European Convention on Human Rights, and deriving from the common constitutional traditions of the Member States, is one of the fundamental rights protected by the legal order the Union. It includes the right of a person to keep his state of health secret.

The transfer to third parties, including to another institution, of personal data relating to the health of a person, collected by an institution, is in itself interference in the private life of the individual, whatever the purpose to which the data so transferred are ultimately put.

However, under Article 8, paragraph 2 of the Convention, the interference with privacy by a public authority may be justified, provided it is "prescribed by law", it pursues one or more aims – exhaustively listed – and it is "necessary" to achieve the aim or aims.

Given the extremely private and sensitive nature of medical data, the possibility to transfer or disclose such information to third parties, even if it is from another institution or another body of the Union, without the consent of the person concerned, calls special scrutiny.

Judgment of the General Court (Second Chamber) of 23 November 2011 – Gert-Jan Dennekamp v European Parliament (Case T-82/09)

As laid down in Article 1 of Regulation No 1049/2001, reflecting Recital 4 of the preamble thereto, that regulation seeks to give the public a right of access to documents of the institutions which is as wide as possible (Joined Cases C-39/05 P and C-52/05 P *Sweden and Turco* v *Council* [2008] ECR I-4723, paragraph 33).

Where an institution is asked to disclose a document, it must assess in each individual case whether that document falls within the exceptions, set out in Article 4 of Regulation No 1049/2001, to the right of public access to documents of the institutions (see, to that effect, *Sweden and Turco* v *Council*, paragraph 21 above, paragraph 35). In view of the objectives pursued by Regulation No 1049/2001, those exceptions must be interpreted and applied strictly (*Sweden and Turco* v *Council*, paragraph 36).

Secondly, it follows from the case-law that, when examining the relationship between Regulation No 1049/2001 and Regulation No 45/2001 for the purposes of applying the exception provided for under Article 4(1)(b) of Regulation No 1049/2001 – namely, the protection of privacy and the integrity of the individual – it must be borne in mind that those regulations have different objectives. Regulation No 1049/2001 is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents and to promote good administrative practices. Regulation No 45/2001 is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private lives, in the handling of personal data (*Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 49).

As Regulation No 1049/2001 and Regulation No 45/2001 do not contain any provisions granting one primacy over the other, the full application of both regulations should, in principle, be ensured (*Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 56).

Article 4(1)(b) of Regulation No 1049/2001 establishes a specific and reinforced system of protection for a person whose personal data could, in certain cases, be communicated to the public (*Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 60).

Where a request based on Regulation No 1049/2001 seeks access to documents including personal data, Regulation No 45/2001 becomes applicable in its entirety, including Article 8 thereof (*Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 63).

Thirdly, it should be noted that, in the present case, the applicant's request for access was made with a view to obtaining the names of the MEPs who were members of the additional pension scheme at the time of the initial request or who had been members of that scheme on 1 September 2005, together with the names of the members of the scheme at the time of the initial request for whom the European Parliament paid a monthly contribution to the scheme. The names of MEPs constitute personal data within the meaning of Article 2(a) of Regulation No 45/2001 (see, to that effect, *Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 68).

Moreover, as the European Parliament correctly found in the contested decision, the communication of personal data falls within the definition of "processing of personal data" used in Regulation No 45/2001 (see, to that effect, *Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 69).

Accordingly, Article 8(b) of Regulation No 45/2001 was applicable to the applicant's request for access, which concerned documents containing personal data, and it is not possible for the applicant to raise against this the argument that the "processing" requested by him was lawful on the basis of Article 5(b) of Regulation No 45/2001 and that this suffices since Article 8(b) of that Regulation applies without prejudice to Article 5.

In order to obtain disclosure of the personal data contained in the documents which he was requesting, the applicant would have had to demonstrate, by providing express and legitimate justifications, the necessity for the requested personal data to be transferred, so that the European Parliament would then have been able to weigh up the various interests of the parties concerned and to determine, as required under Article 8(b) of Regulation No 45/2001, whether there was any reason to assume that the legitimate interests of MEPs might be prejudiced by the transfer of those data (see, to that effect, *Commission* v *Bavarian Lager*, paragraph 13 above, paragraph 78).

Judgment of the Court (Third Chamber) of 24 November 2011 – Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Case C-70/10)

Directives 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society and 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, in conjunction with Directives 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), interpreted in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union having regard to Articles 8 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, are to be interpreted as precluding the adoption by a national court, on the sole basis of a statutory provision providing that "[the competent courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right", to order an "[Internet service provider] to introduce, for all its customers, *in abstracto* and as a preventive measure, exclusively at the cost of [the latter] and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent".

Judgment of the Court (Third Chamber) of 24 November 2011 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado. (Joined cases C-468/10 and C-469/10)

By its first question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest

of the data controller or of the third party or parties to whom the data are disclosed, requires not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources.

Article 1 of Directive 95/46 requires Member States to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their privacy, in relation to the handling of personal data (see, to that effect, Case C-524/06 *Huber* [2008] ECR I-9705, paragraph 47).

In accordance with the provisions of Chapter II of Directive 95/46, entitled "General rules on the lawfulness of the processing of personal data", all processing of personal data must, subject to the exceptions permitted under Article 13, comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the six principles for making data processing legitimate listed in Article 7 of Directive 95/46 (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, paragraph 65, and *Huber*, paragraph 48).

According to Recital 7 in the preamble to Directive 95/46, the establishment and functioning of the internal market are liable to be seriously affected by differences in national rules applicable to the processing of personal data (Case C-101/01 *Lindqvist* [2003] ECR I-12971, paragraph 79).

In that context, it must be noted that Directive 95/46 is intended, as appears from, inter alia, Recital 8 in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. Recital 10 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU (see, to that effect, *Lindqvist*, paragraph 95, and *Huber*, paragraph 50).

Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate (*Lindqvist*, paragraph 96).

Consequently, it follows from the objective of ensuring an equivalent level of protection in all Member States that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful.

That interpretation is corroborated by the term "may be processed only if" and its juxtaposition with "or" contained in Article 7 of Directive 95/46, which demonstrate the exhaustive and restrictive nature of the list appearing in that Article.

It follows that Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7.

The foregoing interpretation is not brought into question by Article 5 of Directive 95/46. Article 5 merely authorises Member States to specify, within the limits of Chapter II of that Directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful.

The margin of discretion which Member States have pursuant to Article 5 can therefore be used only in accordance with the objective pursued by Directive 95/46 of maintaining a balance between the free movement of personal data and the protection of private life (*Lindqvist*, paragraph 97).

Directive 95/46 includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options (*Lindqvist*, paragraph 83). A distinction, consequently, must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 of Directive 95/46, on the one hand, and national measures which provide for a mere clarification of one of those principles, on the other hand. The first type of national measure is precluded. It is only in the context of the second type of national measure that Member States have, pursuant to Article 5 of Directive 95/46, a margin of discretion.

It follows that, under Article 5 of Directive 95/46, Member States also cannot introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7 thereof, nor can they amend, by additional requirements, the scope of the six principles provided for in Article 7.

In the present cases, Article 7(f) of Directive 95/46 provides that the processing of personal data is lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)".

Article 7(f) sets out two cumulative conditions that must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of the personal data must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed; and, secondly, such interests must not be overridden by the fundamental rights and freedoms of the data subject.

It follows that, in relation to the processing of personal data, Article 7(f) of Directive 95/46 precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in the preceding paragraph.

However, account must be taken of the fact that the second of those conditions necessitates a balancing of the opposing rights and interests concerned which depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter).

In this regard, it must be noted that Article 8(1) of the Charter states that "everyone has the right to the protection of personal data concerning him or her". That fundamental right is closely connected with the right to respect for private life expressed in Article 7 of the Charter (Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paragraph 47).

According to the Court's case-law, the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (*Volker und Markus Schecke and Eifert*, paragraph 52). However, it follows from Articles 8(2) and 52(1) of the Charter that, under certain conditions, limitations may be imposed on that right.

Moreover, Member States must, when transposing Directive 95/46, take care to rely on an interpretation of that Directive which allows a fair balance to be struck between the various fundamental rights and freedoms protected by the EU legal order (see, by analogy, Case C-275/06 *Promusicae* [2008] ECR I-271, paragraph 68).

In relation to balancing, which is necessary pursuant to Article 7(f) of Directive 95/46, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental

rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.

Unlike the processing of data appearing in public sources, the processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter must be properly taken into account by being balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed.

In that regard, it must be noted that there is nothing to preclude Member States, in the exercise of their discretion laid down in Article 5 of Directive 95/46, from establishing guidelines in respect of that balancing.

However, it is no longer a precision within the meaning of Article 5 of Directive 95/46 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.

Consequently, without prejudice to Article 8 of Directive 95/46 concerning the processing of particular categories of data, a provision which is not at issue in the main proceedings, Article 7(f) of that directive precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.

In light of those considerations, the answer to the first question is that Article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that those data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

The second question

By its second question, the national court asks, in essence, whether Article 7(f) of Directive 95/46 has direct effect.

In that regard, it must be recalled that, according to settled case-law of the Court, whenever the provisions of a directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may be relied on before the national courts by individuals against the State where the latter has failed to implement that Directive in domestic law by the end of the period prescribed or where it has failed to implement that directive correctly (see Case C-203/10 *Auto Nikolovi* [2011] ECR I-0000, paragraph 61 and the case-law cited).

It must be stated that Article 7(f) of Directive 95/46 is a provision that is sufficiently precise to be relied on by an individual and applied by the national courts. Moreover, while that Directive undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Article 7(f), for its part, states an unconditional obligation (see, by analogy, *Österreichischer Rundfunk and Others*, paragraph 100).

The use of the expression "except where" in the actual text of Article 7(f) of Directive 95/46 is not such, by itself, as to cast doubt on the unconditional nature of that provision, within the meaning of that case-law.

That expression is intended to establish one of the two cumulative elements provided for in Article 7(f) of Directive 95/46 to which the possibility of processing personal data without the data subject's consent is subject. As that element is defined, it does not deprive Article 7(f) of its precise and unconditional nature.

The answer to the second question is therefore that Article 7(f) of Directive 95/46 has direct effect.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

A: Summary of activities and news:

In the course of 2011, the EDPS set new benchmarks in different areas of activity. In the **supervision of EU institutions and bodies**, when processing personal data, the EDPS interacted with more data protection officers in more institutions and bodies than ever before. In addition, the EDPS saw the effects of its new **enforcement policy**: most EU institutions and bodies are making good progress in complying with the Data Protection Regulation, while others should increase their efforts.

In the **consultation of new legislative measures**, the EDPS issued a record number of opinions on a range of subjects. The most prominent is the **Review of the EU legal framework for data protection**, which remains high on the agenda. However, the implementation of the **Stockholm programme** in the area of freedom, security and justice and the **Digital Agenda**, as the cornerstone for the Europe 2020 strategy, also had an impact on data protection. This can also be said of issues in the internal market, public health and consumer affairs, and enforcement in a cross-border context.

At the same time, the EDPS increased **cooperation** with other supervisory authorities and further improved the efficiency and effectiveness of his **organisation** and **communication**.

In 2012, the main priorities for the EDPS include:

- **Raising awareness**: the EDPS will invest time and resources in providing guidance to EU institutions and agencies in the form of thematic guidelines, training and workshops and the development of a dedicated section on the EDPS website for Data Protection Officers (DPOs).

- **Defining procedures** for handling notifications related to standard administrative procedures or to processing operations already in operation.

- An exercise to determine the state of play for DPOs in EU institutions and bodies in order to provide **support for the DPO function** in line with the accountability principle.

- **Visits and inspections** to institutions and agencies, not only for enforcement, but also as a tool to raise awareness of data protection issues and the role of the EDPS.

- In its capacity as advisor, the EDPS will give priority in 2012 to the ongoing work on the **legal framework for data protection in the EU**.

- **Technological developments**, especially those connected to the Internet and associated policies, will be another area of focus. This involves plans for a Pan-European framework for electronic identification, authentication and signature; the issue of Internet monitoring (e.g. enforcement of IP rights, takedown procedures), cloud computing services and eHealth. The EDPS will also strengthen its technological expertise and engage in research on privacy-enhancing technologies.

- Further developing the **Area of Freedom, Security and Justice** (e.g. EU-TFTS, Smart borders) and financial sector reform insofar as they affect the right to privacy and data protection will continue to be followed and scrutinised by the EDPS.

- The EDPS will also continue to fulfil its responsibilities in the field of **coordinated supervision** and reach out to national data protection authorities as well as to international organisations in order to raise awareness and share good practices.

Organisation	European Data Protection Supervisor (EDPS)
Chair and/or College	Peter Hustinx, Supervisor Giovanni Buttarelli, Assistant Supervisor
Budget	EUR 7 564 137
Staff	52 staff members (37 EU officials).
General Activity	
Decisions, opinions, recommendations	**24 legislative opinions** issued on, among others, initiatives relating to the Area of Freedom, Security and Justice, technological developments, international cooperation, data transfers or internal market. **12 sets of formal comments** issued on, among others, intellectual property rights, civil aviation security, EU criminal policy, the Terrorist Finance Tracking System, energy efficiency or the Rights and Citizenship Programme.
Notifications	**164 notifications** of processing operations presenting specific risks received from EU institutions and bodies' Data Protection Officers for prior checking.
Prior checks	**71 prior-check opinions adopted,** notably on health data, staff evaluation, recruitment, suspicion and offences and e-monitoring.
Requests from data subjects	**196 requests for information or advice** received in writing from the general public, mainly on online privacy, international transfers of data, EU data protection framework and data retention.
Complaints from data subjects	**107 complaints received, 26 admissible** Main types of violations alleged: access to and rectification of data, objection and deletion, violation of confidentiality of data, excessive collection and loss of data.
Advice requested by parliament or government	Within the 24 legislative opinions mentioned above, **20** were issued upon request from the European Commission (Article 28(2) of Regulation (EC) No 45/2001).
Other relevant general activity	**34 consultations on administrative measures** related to the

information	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 the EU institutions and bodies.
Inspection activities	
Inspections, investigations	**4 on-the-spot inspections** at the CEDEFOP, OLAF and the ECB. **Follow-up** of recommendations made in previous inspections. **Security audit** of the Visa Information System (VIS).
Sanction activities	
Sanctions	N/A
Penalties	**Monitoring of the implementation of Regulation (EC) No 45/2001**: the third stock-taking exercise has led to a report highlighting the progress made by institutions and bodies in implementing the Regulation and also underlining shortcomings. One-day visits organised at the European Railway Agency, the Community Plant Variety Office, the European Foundation for the Improvement of Living and Working Conditions and the European Global Navigation Satellite Systems Agency.
DPOs	
Figures on DPOs	54 DPOs in EU institutions and bodies.

B. Information on case-law

EDPS participation in court proceedings

In **V. v European Parliament (Case F-46/09)**, the EDPS was invited to intervene by the Civil Service Tribunal. The case concerned the allegedly illegal transfer of medical data between the medical services of the Commission and the European Parliament. The EDPS pleaded in favour of the applicant, arguing that the transfer was contrary to data protection rules, as it was not necessary and lacked a proper legal basis. In its judgment of 5 July 2011, the Civil Service Tribunal ruled in favour of the applicant, following the reasoning of the EDPS.

In its ruling of 7 July 2011, **Valero Jordana v Commission (Case T-161/04)**, the General Court considered that the Commission had been wrong in not assessing the request for public access to certain personal data under the data protection rules. This conclusion was in line with the EDPS's submissions to the Court argument.

In the ruling of 23 November 2011, **Dennekamp v European Parliament (Case T-82/09)**, the General Court concluded that the applicant, a journalist asking for the names of Members of the European Parliament who were participating in an additional pension scheme, had not demonstrated the necessity of having the data made public. The EDPS had defended the opposite view, considering that a balance of the different interests involved should have led to disclosure of the data to the journalist.

The case **Egan & Hackett v European Parliament (Case T-190/10)** has not yet led to a ruling of the General Court. This case concerned a request for access to the names of assistants of Members of the European Parliament.

The EDPS has also intervened in **Commission v Austria (Case C-614/10)**, an infringement case against Austria on the lack of independence of the Austrian data protection authority. The EDPS submitted a statement in intervention, supporting the Commission's conclusion that the way in which the Austrian data protection authority is embedded in the institutional structure of Austria does not sufficiently ensure its independence.

Finally, ENISA brought a case before the General Court against a decision of the EDPS on a **complaint (Case T-345/11)**. The application was declared manifestly inadmissible on procedural grounds.

Data protection case-law

In **Deutsche Telekom (Case C-543/09)** questions were raised on whether under the e-privacy Directive, an undertaking assigning telephone numbers to its subscribers was allowed to provide data relating to these subscribers to another undertaking whose activity consists of providing publicly available directory enquiry services without renewed consent of the persons involved. The Court considered in its ruling of 5 May 2011 that as the subscribers were already correctly informed of this possibility, renewed consent was not needed.

In its ruling in **ASNEF and FECEMD** of 24 November 2011 (**Joined Cases C-648/10 and C-469/10**), the Court of Justice replied to a Spanish court which had asked for clarification on a provision in the data protection Directive, which allows the processing of personal data if this serves a legitimate interest and is not outweighed by the interest of the data subject involved. In Spanish law this was only possible with regard to personal data that had already been made publicly available. According to the Court, this national restriction is not in line with the Directive which has direct effect on this point.

On 24 November 2011, the Court of Justice issued a preliminary ruling in a Belgian case, concerning an obligation on an Internet Service Provider (**Scarlet Extended**) to monitor the Internet behaviour of its customers in order to prevent breaches of intellectual property rights (**Case C-70/10**). The Court concluded that the obligation amounted to a general monitoring obligation which is forbidden under EU rules on e-commerce. The Court also noted that such an obligation would not constitute a fair balance between the enforcement of intellectual property rights and several fundamental rights and freedoms laid down in the Charter on Fundamental rights, amongst which is the right to data protection.

Chapter Four

Principal Developments in EEA Countries

ICELAND

A: Summary of activities and news:

One of the major issues in 2011 was the processing of personal data in relation to anonymous reporting to administrative authorities on alleged law breaches. On the websites of both the Directorate of Labour and the Directorate of Internal Revenue, citizens were given the opportunity to anonymously report their suspicion of tax evasion and related offences. The DPA decided to investigate the lawfulness of processing personal data related to this anonymous reporting. The result of this investigation was published in decisions aimed at the authorities in question, according to which the use of forms for anonymous reporting might, amongst other things; result in inaccurate personal data being collected. Furthermore, the DPA considered guarantees given to those reporting on their anonymity to be unreliable since telecommunications technology entails the possibility of tracking reports to those who sent them, e.g. if a police investigation of wrong accusations is instigated. Even though an administrative authority could never prevent citizens completely from sending anonymous reports, it should, in the light of the aforementioned, not explicitly give them the opportunity to report in that manner. Accordingly, the DPA came to the conclusion that forms for such reports on the websites of the authorities in question were incompatible with the Data Protection Act.

Another major issue was a draft proposal of a new constitution for Iceland, presented by the National Constitutional Committee, which was formed following a national election in 2010. The draft proposal contained a provision on the right to privacy, which was identical to the provision on that right in the existing constitution from 1944. In an opinion on the draft proposal, the DPA drew attention to provisions in recent constitutions and human rights charters, including the Charter of Fundamental Rights of the EU, in which the right to the protection of personal data is specifically stated. The DPA urged the National Constitutional Assembly to add such a statement to its draft proposal. Furthermore, the DPA pointed out that a provision in the draft proposal, according to which everyone had the right to collect and disseminate information, needed to be considered carefully, since the free collection of personal data is nowhere allowed in the western world.

A number of legal acts were passed in 2011 containing provisions on processing personal data. The most significant of them is Act No 68/2011 on Investigative Commissions. According to this Act, the Parliament can appoint commissions for investigating some specific matters. These commissions have, according to the Act, extensive powers, including powers to process personal data. In 2008, an Act was passed on one such commission, i.e. Act No 142/2008 on an Investigation of the Events Leading to, and the Causes of, the Downfall of the Icelandic Banks in 2008, and Related Events. The provisions in Act No 68/2011 are in line with the provisions in this former Act, a description of which can be found in the chapter on Iceland in the 12th Annual Report of the Article 29 Working Party.

Organisation	
Chair and/or College	Sigrún Jóhannesdóttir, Commissioner; Páll Hreinsson, Chairman of the Board of Directors, until November 2011 when Björg Thorarensen became Chairman.
Budget	ISK 69 million (approximately EUR 434 000, according to the exchange rate on 31 December 2011).
Staff	Five legal counsels, one secretary.

General Activity	
Decisions, opinions, recommendations	Approximately 100
Notifications	470
Prior checks	110 processing permits were granted.
Requests from data subjects	Approximately 400
Complaints from data subjects	139
Advice requested by parliament or government	Approximately 50
Other relevant general activity information	In all 1 397 new cases were registered in 2011.
Inspection activities	
Inspections, investigations	14
Sanction activities	
Sanctions	With the exception of daily fines, imposed for each day that the DPA's orders are not obeyed, the DPA does not have sanction power.
Penalties	Daily fines were not imposed in 2011.
DPOs	
Figures on DPOs	N/A

B. Information on case-law:

On 20 October 2011, the Supreme Court of Iceland passed a judgement (case No 706/2010) regarding the publication of a report on a fatal road accident. In the report, the Road Accident Analysis Group described its findings on the causes of this accident, in which the driver was killed. The surviving partner of the driver filed a case, in which he made a claim for compensation for personal injury inflicted on him by the publication of the Group's report, i.e. because the driver's name could easily be deduced from the report even though it was not published. This case had already been handled by the DPA, which considered the driver to be personally identifiable and, accordingly, that the publication of the report entailed processing of personal data. However, in the light of clear legal provisions on the obligation to publish the Group's reports, and because the Group had not published more information in the report than could be considered necessary, the DPA did not find a breach of the Data Protection Act. Both the District Court of Reykjavik and the Supreme Court came to a similar conclusion, i.e. that the Group was legally obliged to publish the report and that the information made public did not constitute an illegal infringement of rights. Accordingly, the plaintiff's claim for compensation was dismissed.

LIECHTENSTEIN

A. Summary of activities and news

Act on a Central Personal Register

A register has been maintained by the regional (federal state) governments for years, which records numerous details of all inhabitants of the state. For years, the data protection office has been calling for a statutory basis for this important database. This call was answered in 2011. An Act was finally passed which also regulates the process for revising the access rights of the individual authorities. The database also needs to undergo certain technical corrections, particularly to ensure that these access rights are appropriate.

Schengen

The data protection evaluation was performed in 2011. The Liechtenstein Data Protection Office (DSS) was audited in respect of its fulfilment of various aspects, such as independence, structure, statutory tasks and competences, as well as the rights of the data subjects. The audit was positive. Liechtenstein has been a member of Schengen since December 2011. Because of a shortage of resources, however, it is hard for it to attend meetings of the Schengen Mixed Committee. An increase in the resources of the DSS was requested during the evaluation. However, this has not been forthcoming.

Public relations work

On the occasion of the European Data Protection Day, the DSS and the Institute of Information Systems at the University of Liechtenstein invited people to attend a public event entitled 'Look who's talking – what mobile phones, laptops etc. can tell us'. Mobile phones, laptops and tablet PCs are impossible to do without these days. Thanks to compact devices and fast wireless networks, we can communicate and work anywhere. So the event focussed on data processing by mobile devices.

At the invitation of the private university in the Principality of Liechtenstein, we participated in a podium discussion on 'State access to private data: the question of data retention'. While data retention has been abolished in Germany by the Federal Constitutional Court, and has not yet been introduced in Austria, in Liechtenstein the traffic and location data of all persons is recorded every time they use their telephone or the internet. The European Data Protection Supervisor describes this considerable encroachment into every citizen's right to privacy as the strongest measure ever taken in the EU to intrude on the private sphere.[19] The advantages and disadvantages of this type of retention were discussed.

On the Networking Day at the University of Liechtenstein, we were invited to a podium discussion about *Cloud Computing*.

In 2009 it became possible to appoint an official or company data protection officer as a substitute for the duty to report data collection activities. In order to create synergies in a still new field, we invited the existing officers and interested parties to share ideas on the subject of 'Tasks and position of a data protection officer'.

[19] Cf. Newsletter January 2011: 'The EDPS regards the Directive as the most privacy-invasive instrument ever adopted by the EU in terms of scale and the number of people it affects': https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_27_EN.pdf and Annual Activity Report for 2010.

The DSS website is the main source of information for the public.[20] Among other things, information about *Cloud Computing* and *Outsourcing* in general has been published here, along with a recommendation to implement *technical and organisational measures to guarantee data security*.

Organisation	
Chair and/or College	Dr Philipp Mittelberger
Budget	CHF 682,000.00
Staff	2.2 Legal, 1.0 Technical, 0.8 Administration.
General Activity	
Decisions, opinions, recommendations	11 approvals for video surveillance systems.
Notifications	N/A; very few new notifications.
Prior checks	N/A
Requests from data subjects	64
Complaints from data subjects	N/A
Advice requested by parliament or government	24 opinions on proposed Acts[21].
Other relevant general activity information	559 enquiries[22]
Inspection activities	
Inspections, investigations	Various controls in preparation.
Sanction activities	
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	25 notified data protection officers by end 2011.

[20] http://www.dss.llv.li/

[21] Cf. DSS Annual Activity Report for 2011, section 3., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.

[22] See DSS statistics, DSS Annual Activity Report for 2011, section 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.

B. Information on case-law

The Data Protection Commission did not publish any decisions in 2011. This may be because it is still unclear as to whether and to what extent the right of appeal under Article 34(b) of the Data Protection Act is actually applied in practice.

In one case before the State Court (Constitutional Court), the right to information on the deceased husband was asserted. The legal basis of this claim was Article 1(7) of the Data Protection Regulation. In connection with the right to information, this provision states: *'If information on deceased persons is requested, it shall be granted if the applicant demonstrates an interest in the information and there are no overriding interests of relatives of the deceased person or from third parties which prevent this. Close kinship, marriage or registered partnership with the deceased person constitute an interest.'*

The State Court began by stating that data protection and the protection of 'informational integrity' are a partial aspect of the protection of privacy under Article 32 of the Liechtenstein Constitution and Article 8 of the European Convention on Human Rights.

It decided in this case that this provision does not establish a separate right to information, but instead has to be seen as a right of access to documents under procedural law. The right to information applies to one's own data. This is not the case in the provision in the Regulation. This is therefore a crucial question of data protection law, which has to be regulated at the level of an Act. The provision therefore has to be interpreted restrictively in line with the constitution, and only (but nevertheless) represents a protected interest in access to documents in actual proceedings (StGH 2011/11).

NORWAY

A. Summary of activities and news

DPA strategy in the health sector

Since 2010 there has been an intern work programme on strategies. In autumn 2011 the "Data strategy for better policy in the health sector" was launched. The Inspectorate has established long-term goals for how the agency will contribute to better policy in the health sector. It includes work around access control (both internal operations and access across), modernisation and coordination of health records (central health records and other quality records), as well as an evaluation of how the Authority can ensure people's self-determination and autonomy. The strategy also addresses how the agency will work to the local quality records, department, Health Directorate, Health and other key stakeholders in the health sector.

Organisation	Norwegian Data protection Authority
Chair and/or College	Director Bjørn Erik Thon
Budget	NOK 32 million
Staff	40 in total, Director: 1, legal: 16, Inspection and Security: 9, Information dep: 4, administration and archive: 10.
General Activity	
Decisions, opinions, recommendations	
Notifications	New in 2011: 4 010, total 11 211 at the end of 2011.
Prior checks	Total in 2011: 143
Requests from data subjects	In total the Norwegian DPA received 5 196 phone calls and 2 632 emails to our front service.
Complaints from data subjects	N/A
Advice requested by parliament or government	N/A
Other relevant general activity information	N/A
Inspection activities	
Inspections, investigations	Address Mediation 1

	Working 3 Customer Card 5 Insurance 4 Research 2 Internet companies 4 Camera surveillance 9 National welfare service 4 Webcast 5 Education 1 TOTAL 38
Sanction activities	
Sanctions	4 penalty fees, and one coercive fee, all by DPA.
Penalties	Penalty fees total NOK 135 000, coercive fines NOK 380 000.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Mapping of Facebook

In December 2010, we launched the report, Social Network Services and Privacy – a case study of Facebook. The report showed that the information that users provide about themselves is only a small part of the total amount of information that Facebook collects. The same report revealed several ambiguities about Facebook's collection and use of personal information. On this basis, the Nordic DPAs sent, on the initiative of the Norwegian Data Inspectorate, a number of specific questions to Facebook about who collects and accesses the information via Facebook, as well as what happens to the personal information collected.

Data Retention Directive

The Norwegian Parliament implemented in April 2011 the Data Retention Directive in Norwegian law. The Directive will be implemented in the electronic communications rules, the Criminal Procedure Act and the Personal Data Regulations.

The DPA will get a number of new duties in relation to the Directive, including supervisory duties relating to the obligation to delete data and to prepare licences with security requirements. The DPA argued strongly against the Directive, but took note of Parliament's decision, and worked together with the Norwegian Post and Telecommunications Authority to secure the best implementation possible. The Directive was not in effect at the end of the year.

App-report

In September 2011, the DPA published the report, What does the app know about you? Privacy challenges related to mobile applications. Mobile applications, called "apps", are growing rapidly. The reason that the audit has looked into this market is that many applications handle large amounts of personal data, often without the user evens being aware of it. Some applications require access to personal information that can reveal a lot about the user, such as where you have been, information about the network of friends and that person's interests.

The RMI case

In 2010, the DPA investigated the Forensic Medicine Institute (RMI) at the University of Oslo. The inspection showed that the department stores large amounts of sensitive data from its activities, without adequate legal basis for such storage either in law or in agreement with each client. The DPA also found that there were major deficiencies in information security for the information and the university in general exercised poor security related to the stored information. During the year the DPA announced that it would decide that the information should be deleted.

"Nettby"

In December 2010, the VG's (Norwegian newspaper) "Nettby" social networking site closed down. Nettby was the largest online community of its time, and significant amounts of information were recorded, including private communications. After the closure, all information present at VG was inaccessible to both their previous users and the public at large. VG and the National Library believed that the information had to be preserved for the future because they reflected that the times we live in now could be interesting for research. The original purpose of Nettby however, was to provide members participation in an online community – including the possibility of private interaction among members. Therefore the DPA imposed deletion.

Industry standard for electronic ticketing

At the initiative of public transport companies, the DPA participated in a collaborative project on privacy-friendly solutions for electronic ticketing and development of an industry standard. An industry standard for electronic ticketing will help to ensure that everyone can travel anonymously by bus, train and boat, and commits the industry to offer electronic tickets that provide good privacy for travellers. The general public should be able to use public transport without disclosing who or where they are, and still get the same benefits and services as commuters who choose to sign personal contracts with a transport company. The Code was launched in December 2011.

Customs control standards for private individuals

The Royal Customs developed a practice whereby information about private individuals' foreign currency transactions was retrieved from the registry, that information would be stored and registered by letter, and the private individuals concerned were requested to submit documentation relating to the relevant transactions and their connection, if any, with customs-related matters. The DPA deemed that this was an investigation of individuals conducted without statutory authority, and ordered Customs to end this practice.

Chapter Five

Members and Observers of the Article 29 Data Protection Working Party

MEMBERS OF THE ART. 29 DATA PROTECTION WP IN 2011

Austria	Belgium
Mrs Eva Souhrada-Kirchmayer (from July 2010) Mrs Waltraut Kotschy (until June 2010) Austrian Data Protection Commission (Datenschutzkommission) Hohenstaufengasse 31 - AT - 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Mr Willem Debeuckelaere Commission for the protection of privacy (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32(0)2/213.85.40 Fax: +32(0)2/213.85.65 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Bulgaria	**Cyprus**
Mr Krassimir Dimitrov Commission for Personal Data Protection –CPDP (Комисия за защита на личните данни) 15 Acad. Ivan Evstratiev Geshov blvd. Sofia 1431 Republic of Bulgaria Tel: + 359 2 915 35 31 Fax: + 359 2 915 35 25 E-mail: kzld@cpdp.bg Website: http://www.cdpd.bg	Mrs Panayiota Polychronidou Commissioner for Personal Data Protection (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) Tel: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy
Czech Republic	**Denmark**
Mr Igor Nemec Office for Personal Data Protection (Úřad pro ochranu osobních údajů)	Mrs Janni Christoffersen Danish Data Protection Agency (Datatilsynet)

Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-mail: posta@uoou.cz Website: http://www.uoou.cz/	Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk
Estonia	**Finland**
Mr Viljar Peep Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) 19 Väike-Ameerika St., 10129 Tallinn Tel: +372 627 4135 Fax: +372 627 4137 e-mail: info@]aki.ee or international@aki.ee Website: http://www.aki.ee	Mr Reijo Aarnio Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tel: +358 10 36 166700 Fax: +358 10 36 166735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
France	**Germany**
Mr Alex Türk Chairman President of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 Mr Georges de La Loyère French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés - CNIL)	Mr Peter Schaar The Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 - DE -53117 Bonn Tel: +49 (0) 228 99-7799-0 Fax: +49 (0) 228 99-7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.datenschutz.bund.de Mr Alexander Dix (representing the German States / Bundesländer)

Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Website: http://www.cnil.fr	The Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragter für Datenschutz und Informationsfreiheit) An der Urania 4-10 – DE – 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Website: http://www.datenschutz-berlin.de
Greece	**Hungary**
Mr Christos Yeraris Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athens - Greece Tel: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Website: http://www.dpa.gr	Mr András Jóri Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: www.adatvedelmibiztos.hu
Ireland	**Italy**
Mr Billy Hawkes Data Protection Commissioner (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tel: +353 57 868 4800 Fax: +353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie	Mr Francesco Pizzetti Italian Data Protection Authority (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it

Latvia	Lithuania
Mrs Signe Plumina Data State Inspectorate of Latvia (Datu valsts inspekcija) Blaumana street 11/13-15 Riga, LV-1011 Latvia e-mail: info@dvi.gov.lv website: www.dvi.gov.lv Tel: + 371 67223131	Mr Algirdas Kunčinas State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Website: http://www.ada.lt
Luxembourg	**Malta**
Mr Gérard Lommel National Commission for Data Protection (Commission nationale pour la Protection des Données - CNPD) 41, avenue de la Gare - L - 1611 Luxembourg Tel: +352 26 10 60 - 1 Fax: +352 26 10 60 - 29 E-mail: info@cnpd.lu Website: http://www.cnpd.lu	Mr Joseph Ebejer Information and Data Protection Commissioner Office of the Information and Data Protection Commissioner 2, Airways House High Street Sliema SLM 1549 Malta Tel: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Website: http://www.idpc.gov.mt
The Netherlands	**Poland**
Mr Jacob Kohnstamm Dutch Data Protection Authority (College Bescherming Persoonsgegevens - CBP) Visiting address (only with an appointment):	Mr Wojciech Rafał Wiewiórowski Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw

Juliana van Stolberglaan 4-10 2595 CL DEN HAAG Postal address: P.O. Box 93374 2509 AJ DEN HAAG Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl	Tel: +48 22 860 7312; +48 22 860 70 81 Fax: +48 22 860 73 13 E-mail: desiwm@giodo.gov.pl Website: http://www.giodo.gov.pl
Portugal	**Romania**
Mr Luís Novais Lingnau da Silveira National Commission of Data Protection (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-mail: geral@cnpd.pt Website: http://www.cnpd.pt	Mrs Georgeta Basarabescu National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E-mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro
Slovakia	**Slovenia**
Mr Gyula Veszelei Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441	Mrs Natasa Pirc Musar Information Commissioner (Informacijski pooblaščenec) Vošnjakova 1, SI - 1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78

E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	E-mail: gp.ip@ip-rs.si Website: http://www.ip-rs.si rs.si
Spain	**Sweden**
Mr José Luis Rodriguez Álvarez Spanish Data Protection Agency (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6219/20 Fax: +34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Mr Göran Gräslund Data Inspection Board (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
United Kingdom	**European Data Protection Supervisor**
Mr Christopher Graham Information Commissioner's Office Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-mail: please use the online enquiry form on our website Website: http://www.ico.gov.uk	Mr Peter Hustinx European Data Protection Supervisor - EDPS Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 63, BE - 1047 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

OBSERVERS OF THE ART. 29 DATA PROTECTION WORKING PARTY IN 2011

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

Samoilova 10, 1000 Skopje, RM Tel: +389 2 3230 635 Fax: +389 2 3230 635 E-mail: info@dzlp.mk Website: www.dzlp.mk	

Secretariat of the Art. 29 Working Party
Mrs Marie-Hélène Boulanger Head of unit European Commission Directorate-General Justice Data Protection Unit Office: MO59 02/13 - BE - 1049 Brussels Tel: +32 2 295 12 87 Fax: +32 2 299 8094 E-mail: JUST-ARTICLE29WP-SEC@ec.europa.eu Website: http://ec.europa.eu/justice/data-protection/index_en.htm

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

DS-AA-14-001-EN-N

Publications Office

doi: 10.2838/10852