European Commission

Sixteenth Report

of the Article 29 Working Party on Data Protection

Covering the year 2012

Adopted on 25 November 2014

Justice and consumers

Luxembourg: Publications Office of the European Union, 2015

PDF	ISBN 978-92-79-44096-0	2363-099X	10.2838/83967	DS-AA-15-001-EN-N

Sixteenth Report of the Article 29 Working Party on Data Protection

Covering the year 2012

Table of Contents

INTRODUCTION BY THE CHAIRMAN 1
ISSUES ADDRESSED BY THE ARTICLE 29 DATA PROTECTION WORKING PARTY 2
1.1. Transfer of data to third countries 3
1.1.1Adequacy 3
1.1.2 Binding Corporate Rules (BCR) 4
1.2 Electronic communications, internet and new technologies 4
1.3 Revision of the data protection legal framework 8
1.4. Personal data 11
1.4.1 epSOS 11
1.4.2 Developments in biometric technologies 12
MAIN DEVELOPMENTS IN MEMBER STATES 14
Austria 15
Belgium 19
Bulgaria 23
Cyprus 29
Czech Republic 32
Denmark 35
Estonia 38
Finland 39
France 42
Germany 52
Greece 56
Hungary 60
Ireland 65
Italy 67
Latvia 72
Lithuania 76
Luxembourg 79
Malta 82
Netherlands 85
Poland 88
Portugal 94

Romania 96
Slovakia 100
Slovenia 105
Spain 111
Sweden 115
United kingdom 117
EUROPEAN UNION AND COMMUNITY ACTIVITIES 122
3.1. European Commission 123
3.2 European Court of Justice 121
3.3. European Data Protection Supervisor 130
PRINCIPAL DEVELOPMENTS IN EEA COUNTRIES 134
Iceland 135
Liechtenstein 138
Norway 140
MEMBERS AND OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WP 143
Members of the Art. 29 Data Protection WP in 2012 144
Observers of the Art. 29 Data Protection WP in 2012 149

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

The year 2012 promised to be a very important year for data protection in the European Union and a very interesting one for the Article 29 Working Party. In 2012 the European Commission would present its proposals for the new legal framework in the EU on data protection. Considering in 2009 the Working Party had already started to provide the Commission with input for this new legal framework, the presentation of the proposals would be a very important moment.

And in January 2012 the European Commission did indeed present its proposal for a new legal framework on data protection in the EU, consisting of a general data protection Regulation and a Directive applicable to the law enforcement sector.

In general, the proposal was very much welcomed by the Working Party. The fact that the instrument of a Regulation had been chosen, which is directly applicable in all Member States of the EU, is a big step forwards. Even though the proposal consists of two different instruments, comprehensiveness can still be ensured by the legislature, provided it deals with the Regulation and the Directive as a package and the basic principles and rights are the same in both instruments.

Naturally, there are also some remaining concerns. For example, the Working Party feels that the principle of purpose limitation, which is one of the basic principles of data protection, could seriously be undermined by the introduction of the provision that stated that if a new legal ground could be found, the data could be used for a different - also incompatible - purpose. Naturally, sometimes it must be able to use data for other purposes; however these must be compatible with the purpose for which the data was first collected. Simply seeking a different legal ground is not enough.

Notwithstanding the role of the Commission as guardian of the Treaties, there are strong reservations with regard to the role foreseen for the Commission, as many of the provisions could result in encroaching upon the independent position of DPAs. When a matter is being dealt with, or has been dealt with, by the EDPB under the consistency mechanism, the Commission should be able to provide its legal assessment but should in principle refrain from interference.

Furthermore, leaving certain issues to delegated and/or implementing acts may naturally be necessary. However, not all issues for which a delegated or implementing act are foreseen are suitable to be dealt with in such instruments. In some instances the matter concerned is not a detail and should be taken up in the text of the Regulation itself, while in other instances a more appropriate instrument would be guidance by the European Data Protection Board (EDPB).

After the presentation of the proposal the European Parliament (EP) and the Council started their respective legislative procedures. At the time of writing the responsible committee of the European Parliament (LIBE) has finished its discussions and adopted its position on the basis of which the EP will enter the negotiations. In the Council however, discussions are still ongoing.

Technical developments and the increasing globalisation of our society has made it more and more necessary to update the data protection legal framework in the EU and make it fit for the future.

Therefore, the discussions in the Council will hopefully soon lead to a common position of the Member States, ensuring that the negotiations - or trialogue - can commence shortly, aiming to have a new legal framework adopted in the summer of 2014.

Jacob Kohnstamm.

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

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

1.1. TRANSFER OF DATA TO THIRD COUNTRIES

1.1.1 Adequacy

Opinion 7/2012 (WP198) on the level of protection of personal data in the Principality of Monaco

In 2009 the Principality of Monaco requested the Commission to assess whether it offered an adequate level of protection of personal data within the meaning of Article 25(6) of Directive 95/46/CE, and to proceed to a Commission decision in that regard. As part of the adequacy procedure, the Commission requested the opinion of the Article 29 Working Party.

Due to historical links between France and Monaco, Monaco data protection legislation is similar to French data protection law. Article 20 of the Monaco Constitution confirms the protection of the right to privacy, and provides that 'Everyone has the right to respect for his private and family life and the secret of his correspondence'.

The protection of personal data in Monaco is regulated by Act No 1.165 of 23 December 1993 on the protection of personal data (amended by Act No 1.353 of 4 December 2008 and Act No 1.353 of 1 April 2009), and by Sovereign Ordinance No 2.230 of 29 June 2009, which sets out the implementing conditions of the Act.

The assessment of the Working Party essentially relates to Act No 1.165 as amended in 2008 and 2009, by reference to the main provisions of the Directive, and taking into account the guidelines it had set out in its Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive, adopted on 24 July 1998 (WP 12).

The Act establishes the data protection authority of Monaco, the Commission de Contrôle des Informations Nominatives (CCIN) as an independent authority. The CCIN has issued guidelines, deliberations, annual reports and published other information on various subjects such as biometrics, GPS chips, video surveillance and others, setting out the rights and duties of individuals, businesses and the State, and providing guidance on the practical application of privacy principles.

In the international sphere, Monaco signed and ratified the European Convention on Human Rights in 2005, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol (in force since 1 April 2009) as well as the International Covenant on Civil and Political Rights on 28 August 1997.

The Working Party considered that the scope of the Monaco legislation was similar to that set out in the Directive, although it felt that adjustments to the wording would clarify its applicability to legal persons.

The Working Party was of the opinion that the legislation met the requirements of the data quality principle and proportionality principle, the transparency principle and the security principle, as well as with the rights of access, rectification and opposition, provided that exceptions were interpreted strictly.

Monaco legislation was seen to comply with the onward transfer principle, and, generally, with the requirements relating to special categories of data.

Although the provisions regarding the right to oppose in the case of direct marketing could have been set out more clearly, sufficient safeguards were in place in this regard. The legislation was also considered to comply with the 'automated individual decision principle'.

The Working Party considered that the objective to deliver a good level of compliance with rules was achieved only in part, and suggested adopting provisions on more effective implementation of the structural and financial independence of the CCIN, as well as to enhance the enforcement powers vested in the authority as regards compliance by the public sector and, more generally, increase the range of

measures that can be imposed on data controllers that fail to comply with the law over and above mere imposition of criminal penalties by judicial authorities.

The Working Party considered that Monaco legislation offered sufficient mechanisms to provide assistance and support to individuals, and sufficiently guaranteed the right of the data subject to be compensated for any damage infringing upon his/her rights or property as a consequence of the illegal processing of his personal data.

The Working Party concluded that the Principality of Monaco guaranteed an adequate level of protection of personal data within the meaning of Article 25 (6) of Directive 95/46/EC, but suggested including concepts such as 'filing system', 'third party', 'processor' and 'data subject consent'; clarifying the applicability of the law to legal persons; clarifying the right for data subjects to be informed in a timely manner (especially where data were not obtained directly from the data subject) and to object to processing for direct marketing purposes. The enforcement powers of the authority should also be improved as regards compliance by the public sector and the measures that can be imposed on data controllers for illegal processing.

1.1.2 Binding Corporate Rules (BCR)

Working Document 2/2012 (WP 195) setting up a table with the elements and principles to be found in Processor Binding Corporate Rules

The Article 29 Working Party previously developed tools to facilitate the use of Binding Corporate Rules (BCR) for Controllers in BCR for your own data (WP 153), intended to regulate the transfers of personal data that are originally processed by the company as Controller (such as data relating to its customers, its employees, etc.).

The aim of this document is to develop a toolbox, describing the conditions to be met, to facilitate the use of Binding Corporate Rules (BCR) for Processors (BCR for third-party data).

BCR for Processors intend to govern international transfers of personal data that are originally processed by a company as the data processor in accordance with external instructions given by a data controller (such as outsourcing activities). According to Directive 95/46/EC, a contract should be signed between a controller and a processor. This contract is referred to in this document as the 'service agreement'.

Recommendation 7/2012 (WP 195a) on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities

In conjunction with the toolbox developed for Binding Corporate Rules for Processors, with this recommendation, the Working Party adopted a standard application form for the approval of processing pursuant to such Binding Corporate Rules.

1.2 ELECTRONIC COMMUNICATIONS, INTERNET AND NEW TECHNOLOGIES

Opinion 6/2012 (WP 197) on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications

This opinion is on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications which, for technical reasons, was first a draft Commission Decision, and subsequently a Regulation.

In its opinion, the Working Party welcomes the Commission's detailed effort to clarify the personal data breach provisions of Directive 2002/58/EC, but suggests that some of the terms used could be expressed with more precision.

As regards **notification to the competent authority**, the Working Party welcomes the fact that specific deadlines are included in the Regulation, and supports the two-step notification scheme that allows combining responsiveness and comprehensiveness.

As regards **information to be provided and initial notification**, the Working Party considers that, in order to stimulate providers in implementing a high-quality personal data security policy, the provider should be asked to provide all the details of which it is aware during the first notification phase, including the type of personal data that is concerned, the circumstances of the breach or type of exposure (loss, theft, copying, etc.) and how the breach was detected (detection software in place, analysis of the logs, an employee reported an incident, etc.).

As regards **electronic means**, the Working Party supports the initiative to promote such means when possible, but warns that the implementation of these electronic means across Member States is not immediate: it will be necessary to define a common electronic notification format, adopt adequate security measures, and develop and test the electronic means (portal and/or another system such as secure e-mail) that will support this mechanism in each Member State.

As regards **notification to the other national authorities concerned**, the Working Party welcomes and supports active cooperation between authorities and clearly understands the need for cooperation between competent national authorities, but advises the Commission to specify the scope of the relevant provision and clarify the practical ways in which competent authorities should cooperate.

As regards **notification to the subscriber or individual** authority, the Working Party welcomes that the Regulation describes a procedure in cases where the persons cannot be reached directly. The Working Party also welcomes the description of the circumstances to be taken into account when assessing whether a breach adversely affects the personal data or privacy of a subscriber or individual.

As regards **assessing severity and adverse effects**, the Working Party has identified the necessity for uniform and easily understandable severity assessment methodology for both providers and competent authorities in Europe. The Decision would strongly benefit from more detailed guidelines in this respect. To address this requirement, the Working Party strongly supports the establishment of a pan-European harmonised severity assessment methodology based on objective criteria.

As regards **technological protection measures and unintelligibility of data**, the Working Party welcomes such measures and believes that they will drive stakeholders towards stronger security practices while providing stronger legal certainty on the notion of unintelligible data across Member States. However, this Regulation should not create the impression that implementing encryption, hashing or secure deletion is sufficient by itself to allow providers to claim that they have fulfilled the general security obligation in Article 17 of Directive 95/46/EC — providers also need to implement adequate organisational and technical measures to prevent, detect and block personal data breaches.

Otherwise the Working Party notes that the draft Regulation does not include any provision or recital regarding the inventory mentioned in Article 4(4) of the Directive. Considering the tight links between the notifications and the inventory, the Working Party suggested adding a Recital in the Decision to mention that providers may also refer to the Regulation to determine the format of the inventory entries. Similarly, the draft Regulation provides that authorities maintain statistics about breaches. The Working Party suggests including a harmonised set of indicators to be monitored statistically.

Opinion 5/2012 (WP 196) on Cloud Computing

In this Opinion the Article 29 Working Party analyses all relevant issues for cloud computing service providers operating in the European Economic Area (EEA) and their clients, specifying all applicable

principles from Directive 95/46/EC and the E-privacy Directive 2002/58/EC (as revised by Directive 2009/136/EC) where relevant.

Despite the acknowledged benefits of cloud computing, the Opinion outlines how the wide scale deployment of cloud computing services can create data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider.

This Opinion examines issues associated with the sharing of resources with other parties, the lack of transparency of an outsourcing chain consisting of multiple processors and sub-contractors, the unavailability of a common global data portability framework and uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA. Similarly, a lack of transparency in terms of the information a controller is able to provide to a data subject on how their personal data is processed is highlighted in the Opinion as matter of serious concern. Data subjects must be informed about who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect.

A key conclusion of this Opinion is that businesses and administrations wishing to use cloud computing should conduct a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services.

The Working Party welcomes Article 26 of the Commission's proposed draft Regulation aimed at making processors more accountable towards controllers by assisting them in ensuring compliance in particular with security and related obligations. Article 30 of the proposal introduces a legal obligation for the processor to implement appropriate technical and organisational measures. The draft proposals clarify that a processor failing to comply with the controller's instructions qualifies as a controller and is subject to specific joint controllership rules.

The Working Party considers that the proposal goes in the right direction to remedy the imbalance in the cloud computing environment, where a client (especially an SME) may find it difficult to exercise the full control required by data protection legislation on how the provider delivers the requested services. Furthermore, in view of the asymmetric legal position of data subjects and small business users *vis à vis* big cloud computing providers, a more proactive role for consumer and business interest organisations is recommended in order to negotiate more balanced general terms and conditions of such companies.

The Working Party considers that, in the interests of legal certainty for the data subjects whose personal data are stored in data centres all over the world, the draft Regulation should include a prohibition on controllers operating in the EU from disclosing personal data to a third country if so requested by a that country's judicial or administrative authority unless this is expressly authorised by an international agreement or approved by a supervisory authority.

Public bodies should first assess whether the communication, processing and storage of data outside the national territory may expose the security and privacy of citizens and national security and the economy to unacceptable risks - in particular if sensitive databases (e.g. census data) and services (e.g. healthcare.) are involved. From this standpoint, consideration might be given by national governments and European Union institutions to further investigate the concept of a European governmental cloud as a supranational virtual space where a consistent and harmonised set of rules could be applied.

The Working Party supports the idea of a European Cloud Partnership which involves public IT procurement to stimulate a European cloud market. Transferring personal data to a European cloud provider governed by European data protection law could bring data protection advantages to customers, in particular by

fostering the adoption of common standards (especially in terms of interoperability and data portability), as well as legal certainty.

Opinion 4/2012 (WP 194) on Cookie Consent Exemption

Article 5.3 of Directive 2002/58/EC, as amended by Directive 2009/136/EC has reinforced the protection of users of electronic communication networks and services by requiring informed consent before information is stored or accessed in the user's (or subscriber's) terminal device.

The requirement applies to all types of information stored or accessed in the user's terminal device. This opinion explains how the revised Article 5.3 impacts on the usage of cookies but the term should not be regarded as excluding similar technologies.

Article 5.3 allows cookies to be exempted from the requirement of informed consent, if they satisfy one of the following criteria: the cookie is used 'for the sole purpose of carrying out the transmission of a communication over an electronic communications network', or the cookie is 'strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'.

While the requirements for informed consent have already been examined in detail by the Working Party, this aim of this document is to analyse the exemptions to this principle in the context of cookies and related technologies.

The analysis conducted by the Working Party suggests that the following cookies can be exempt from the requirement for informed consent under certain conditions if they are not used for additional purposes: user input cookies, for the duration of a session or persistent cookies limited to a few hours in some cases; authentication cookies, used for authenticated services, for the duration of a session; user-centric security cookies, used to detect authentication abuses, for a limited persistent duration; multi-media content player session cookies, such as flash player cookies, for the duration of a session; load-balancing session cookies, for the duration of session; UI customisation persistent cookies, for the duration of a session (or slightly more); and third-party social plug-in content-sharing cookies, for logged in members of a social network.

As regards social networks, the Working Party notes that the use of third-party social plug-in cookies for purposes other than to provide a functionality explicitly requested by their own members requires consent, notably if these purposes involve tracking users across websites.

The Working Party recalls that third-party advertising cookies cannot be exempted from consent, and further clarifies that consent would also be needed for operational purposes related to third-party advertising such as frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging. While some operational purposes might certainly distinguish one user from another, in principle these purposes do not justify the use of unique identifiers. This point is of particular relevance in the context of the current discussions regarding the implementation of the Do Not Track standard in Europe.

This analysis also shows that first-party analytics cookies are not exempt from consent but pose limited privacy risks, provided reasonable safeguards are in place, including adequate information, the ability to opt-out easily and comprehensive anonymisation mechanisms.

Ultimately, to decide if a cookie is exempt from the principle of informed consent it is important to carefully verify if it fulfils one of the two exemption criteria defined in Article 5.3 as modified by Directive 2009/136/EC. After a careful examination, if substantial doubts remain on whether or not an exemption criterion applies, website operators should closely examine if there is not in practice an opportunity to gain consent from users in a simple unobtrusive way, thus avoiding any legal uncertainty.

Opinion 2/2012 (WP 192) on facial recognition in online and mobile services

There has been a rapid increase in the availability and accuracy of facial recognition technology in recent years which has been integrated into online and mobile services for the identification, authentication/verification or categorisation of individuals. This technology is available for use by both public and private organisations. Examples of use in online and mobile services include social networks and smart phone manufacturers.

The ability to automatically capture data and recognise a face from a digital image has been considered previously by the Working Party in the Working document on biometrics (WP80) and Opinion 03/2012 (WP193) on developments in biometric technologies. Facial recognition is considered within the scope of biometrics as, in many cases, it contains sufficient detail to allow an individual to be uniquely identified.

In this opinion the Working Party considered the legal framework, and provided recommendations applicable to facial recognition technology when used in the context of online and mobile services. The opinion is aimed at European and national legislative authorities, data controllers and users of such technologies, and builds upon the principles set out in Opinion 03/2012 within the scope of online and mobile services.

The Working Party concluded that the risks to privacy from a facial recognition system depend on the type of processing involved, and the purpose(s), and made recommendations regarding specific risks.

Images may only be acquired in an online setting if there is a legal basis.

Digital images and templates should only be used for the specific purpose for which they have been provided, and there should be technical controls to reduce the risk that digital images are further processed by third parties for purposes to which the user has not consented.

Data controllers should ensure the security of data transit between image acquisition and the remaining processing stages (e.g. uploading an image from a camera to a website for feature extraction and comparison), either by encrypted communication channels or encrypting the acquired image itself.

Data controllers should ensure that templates generated by a facial recognition system contain no more data than necessary to perform the specified purpose, thereby avoiding any possible further processing. Templates should not be transferrable between facial recognition systems.

Since identification and authentication/verification were likely to require the storage of the template for use in a later comparison, the Working Party recommended that data controllers consider the most appropriate location for storage of the data, whether on the user's device or within the data controller's systems. Data controllers should ensure the security of the data stored, by encrypting the template if necessary, so as to prevent unauthorised access to the template or storage location. In the case of facial recognition for the purpose of verification, biometric encryption techniques are advised.

Finally, the Working Party recommended that data controllers should provide data subjects with appropriate mechanisms to exercise their right of access, where appropriate, to both the original images, and the templates generated in the context of facial recognition.

1.3 REVISION OF THE DATA PROTECTION LEGAL FRAMEWORK

Opinion 1/2012 (WP 191) on the data protection reform proposals

In general, the Regulation provides greater clarity. It strengthens individuals' rights including more transparency, greater control over processing, data minimisation, specific provisions for processing children's personal data, strengthened rights to data access, strengthened rights to object, rights to data portability, strengthened rights to data deletion (the 'right to be forgotten') and strengthened rights to redress both through the DPA and the courts.

For data controllers the Regulation brings simplification and greater consistency, a stronger focus on their accountability for data processed and the need to demonstrate this through data protection by design, data protection by default, privacy impact assessments, the appointment of a DPO, data-breach notification duties and the adoption of a precautionary approach to international transfers. In addition, Binding Corporate Rules are expressly recognised as a tool to frame international transfers.

For data processors, data security obligations are given a legal basis, and an obligation is introduced to take on the responsibility of controller for specific data processing operations if the processor goes beyond the instructions of a controller regarding that processing operation (relevant to 'cloud' providers).

For DPAs the Regulation provides for strengthened independence and powers, including administrative fines and the obligation to be consulted on legislative measures, and provisions to ensure harmonised application and where necessary enforcement of the law, especially through the 'consistency mechanism'.

The Working Party has serious reservations with regard to the extent that the Commission is empowered to adopt delegated and implementing acts, which is especially relevant because a fundamental right is at stake, as well as the Commission's role in the European Data Protection Board.

The Working Party suggests conducting an independent in-depth assessment of the increased costs for DPAs and the EDPS (as secretariat for the EDPB) based on the current proposals.

Generally, in relation to the draft Regulation, the Opinion covers horizontal issues such as the role of the Commission, the role of European Data Protection Authorities in policy-making, thresholds for SMEs, implications on budget and resources, general provisions (*scope*, *data subject and personal data*, *biometric data*, *main establishment, pseudonymisation, data protection by design and data protection by default),* the principle of public access to information, further incompatible use, exceptions introduced for public authorities, minors, the right to be forgotten, direct marketing, profiling, representatives, accountability, data-breach notification, the role and functioning of DPAs (*independence*, *powers*, *budget*, *margin of discretion),* jurisdiction and the competence of DPAs (one-stop shop), mutual assistance, consistency (*application of national law (Chapter IX)*, *deadlines),* 'One-stop shop' for data subjects, EDPB institutional structure, international transfers, disclosures not authorised by EU law, the right to liability and compensation, fines, judicial remedies, and churches and religious associations.

The Working Party notes the explicit choice of the European Commission not to present one single instrument for data protection across the board, and to present a Directive as the instrument to regulate data protection in the area of police and criminal justice at the high, consistent level of data protection at which it is aiming.

The Working Party regrets that the provisions related to the powers of DPAs are not very detailed, nor in line with those included in the Regulation. Specifically, the Directive does not include provisions relating to access to premises as is provided for under the Regulation. The ability for the regulator to access the premises of the data controller when necessary should apply to all sectors.

The Working Party regrets that the Directive does not contain provisions on the establishment of time limits, review and other safeguards as the limitation of use of data for serious crimes etc. The Working Party notes that there is no obligation for the competent authorities that have transmitted data to inform the recipient that the transmitted data were incorrect or unlawfully transmitted.

The Working Party finally regrets that the Directive does not contain a provision on the transfer to private parties or other authorities, which are not a competent authority under the Directive. The Working Party therefore urges the European legislator to introduce a provision, allowing for transfers of law enforcement data to private parties only in the narrowly defined circumstances defined by law.

With regard to the Directive, the topics addressed are the choice of instrument, consistency, scope of application, data processing principles, data subject rights, data controller obligations, international transfers (*general principles for transfers and onward transfers*, *negative adequacy decisions*, *transfers by way of appropriate safeguards* and *derogations)* and the powers of DPAs and co-operation.

Opinion 8/2012 (WP 199) providing further input on the data protection reform discussions

In its opinion of 23 March 2012, the Article 29 Working Party provided its first general reaction to the Commission proposals, highlighting areas of concern and making certain suggestions for improvement. With a view to the ongoing discussions in both the European Parliament and the Council, the Working Party decided to adopt this opinion providing further guidance, notably on certain key data protection concepts and by analysing the need for, and the effect of, the proposed delegated acts and where necessary suggesting more suitable alternatives.

The key concepts were those of the definition of personal data and the notion of consent.

On the proposed delegated acts, the Working Party expressed its views on the necessity or otherwise of such acts by reference to specific provisions of the proposal.

In relation to Article 14(7) for further specifying various criteria for categories of recipients, notice of potential access, further information for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions, the Working Party allowed that such conditions could be laid down by a delegated act, but more detailed guidance from the EDPB could help with assessing cases in which controllers could invoke the exemption, based on an analysis of various practical situations and contexts.

As for Article 15(3) for further specifying the criteria and requirements for the communication to the data subject of the content of the personal data undergoing processing and of any available information as to their source, no further legislation or guidance was considered to be necessary.

As regards Article 17(9) specifying the criteria and requirements for the right to be forgotten for specific sectors and in specific data processing situations and the conditions for deleting links, copies or replications of personal data from publicly available communication services, the Working Party agreed that a delegated act was the most appropriate method if it was adopted at the same time that the Regulation entered into force. The same applied for Article 20(5), specifying criteria and conditions for suitable measures to safeguard the data subject's legitimate interests, if there was additional guidance from the EDPB.

No guidance by means of delegates acts was deemed necessary for the criteria and requirements in Articles 8 (consent requirements), 12 (excessive fees and requests), 22 ('general accountability' Article), 26 (choosing a processor), or 28 (maintaining documentation).

Guidance issued by the EDPB was regarded as the preferable option for further specifying criteria and requirements in Articles 6 (legal basis), 9 (sensitive data), 23 and 30 (security of processing) and 34 (prior checking).

Considering their importance for all stakeholders, the criteria and requirements in Articles 31 and 32 (obligation to notify a data breach), as well as Article 83, should have been dealt with in the text of the Regulation itself, at least relating to the main lines. For some details, a delegated act would do, if it was adopted at the same time as the Regulation entered into force.

Delegated acts, with additional guidance from the EDPB, were thought appropriate for specifying the criteria and requirements in Articles 33, 35, 37 and 44(1)(h).

The actions referred to in Articles 39 (certification), 79 (fines), 81 and 82 (delegated acts) were considered sufficient.

1.4. PERSONAL DATA

1.4.1 epSOS

Working Document 1/2012 (WP 189) on epSOS

The objective of this Working Document of the Article 29 Working Party is to provide guidance on data protection issues in relation to the epSOS (European Patients Smart Open Services) project, clarifying the most important principles of Directive 95/46/EC, and explaining how the Working Document on the processing of personal data relating to health in electronic health records (WP 131) applies to the epSOS project.

EpSOS is a large-scale pilot project concerning electronic patient record systems in the context of two cross-border services: patient summary and e-prescription.

In its assessment, the Working Party arrived at a number of conclusions.

All data contained in medical documentation, in electronic health records and in HER systems are 'sensitive personal data' and are therefore subject to Article 8 of the Directive. The processing of healthcare data must have a clear legal basis.

One of the basic preconditions for valid consent is that the information given to the data subject satisfies the requirements of Articles 10 and 11 of the Directive.

The processing of personal data must be strictly limited to the minimum which is necessary for the fulfilment of the epSOS purposes, which must be specified, explicit and legitimate. In order to safeguard that data are not kept longer than is necessary in the epSOS system, a maximum retention period should be decided, as well as a common procedure as to what shall happen to the data at the end of the retention period.

Each query about the personal data available through epSOS should be for a real need of access to specific information related to the care or treatment to be provided or the medicine to be prescribed or dispensed in a particular case.

Because of the cross-border character of the epSOS processing, co-operation between DPAs in supervising epSOS is strongly recommended.

All data controllers handling epSOS data must notify the competent supervisory authority in accordance with the national legislation, regardless of whether the data subjects are nationals or residents of another Member State, and irrespective of whether the data handled originate from data controllers in other Member States.

A high level of IT security is necessary for epSOS, including the following: staff implementing the project should have clear, written instructions on the appropriate use of the epSOS system in order to prevent security risks and breaches; suitable arrangements should be made in using the patient summary and e-prescription storage and archiving systems to protect the data against unauthorised access, theft and/or partial/total loss of storage media; for data exchanges, secure communication protocols and end-to-end-encryption must be adopted based on the encryption standards for securing electronic communications; special attention must be paid to reliable and effective electronic identification systems that provide authentication (of both participating staff and patients); the system must be capable of correctly recording and tracking, in an auditable way, the individual operations that make up the overall data processing; unauthorised data access and/or changes should be prevented when the back-up data are transferred and/or stored (e.g. by means of encryption); with regards to the e-prescription system, additional measures should be deployed in order to ensure that pharmaceutical operators can only access digital prescriptions for providing the medicines prescribed; and in emergency situations, any access should be logged and subject to audit.

All data controllers who handle epSOS data must provide data subjects with the right of access to and rectification/erasure/blocking of their own data, and a data subject should be able to address questions

about access and demands for rectification/erasure/blocking to any of the controllers, as well as to any other body involved in the exchange of information within epSOS. A demand for access or rectification/erasure/blocking made to an epSOS partner who does not handle data about the data subject should be forwarded to the data controller in charge within the epSOS system even if this controller is established in another Member State.

epSOS should consider granting the data subject direct (electronic) reading access to his/her own data. A common epSOS website should be constructed to inform on the specific rights of data subjects according to the respective legal frameworks of the participating states.

1.4.2 Developments in biometric technologies

Opinion 3/2012 (WP193) on developments in biometric technologies

Previously, in its Working document on biometrics (WP80) of 2003, the Working Party explored the data protection questions related to the use of upcoming technologies that electronically read and processed biometric data.

In the subsequent years the use of this technology has grown widely, and new emerging services have developed. Biometric technologies that once needed significant financial or computational resources have become dramatically cheaper and faster. These technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition, many of them allow for automated tracking, tracing or profiling of persons, and as such, their potential impact on the privacy and the right to data protection of individuals is significant.

In this opinion, The Working Party provides a revised and updated framework of unified general guidelines and recommendations on the implementation of privacy and data protection principles in biometric applications. The opinion is aimed at European and national legislative authorities, the biometric systems industry and users of such technologies.

Biometric systems rely on several actors: manufacturers, integrators, resellers, installers, clients and data subjects. Security should be a primary concern because biometric data are irrevocable. The Working Party recommends a high level of technical protection for the processing of biometric data, using the latest technical possibilities. In this regard, the Working Party recommends following industry standards for the protection of the systems in which biometric information are processed.

Privacy by design is the concept of embedding privacy proactively into technology itself. Regarding biometric systems, Privacy by design concerns the whole value chain of biometric systems. The Working Party recommends that biometric systems are designed according to formal 'development lifecycles' which include specification of requirements based on a risk analysis and/or a dedicated Privacy; description and justification on how the design fulfils the requirements, validation with functional and security tests, and verification of compliance of the final design with the regulatory framework.

A Privacy Impact Assessment (PIA) is a process in which an entity carries out an evaluation of the risks associated with a processing of personal data and a definition of additional measures designed to mitigate these risks. It should take into account the nature of the collected information, the purpose of the collected information, the accuracy of the system, the legal basis and legal compliance, access to the device and the internal and external sharing of information within the data controller, which will imply security techniques and procedures to protect personal data unauthorised access, less privacy-invasive measures already taken, the decisions taken regarding retention time and deletion of data, and data subjects' rights.

Biometric data require specific attention because they unambiguously identify individuals by using their unique behavioural or physiological characteristics. For this reason, PIAs should aim to assess how identity fraud, purpose diversion and data breach can be avoided or substantially limited by the system it analyses.

On account of their nature, the processing of biometric data requires special technical and organisational measures and precautions to prevent adverse effects to the data subject in the event of a data breach.

Technical measures, especially where large biometric databases are used, could include biometric templates, storage on a personal device vs centralised storage, renewable and revocable identity links, encrypted form, anti-spoofing, biometric encryption and decryption, and automated data erasure mechanisms.

Organisational measures could include requiring the data controller to establish a clear procedure on who can access the information on the system, if the access is partial or not, and ensuring that all actions are tracked.

Chapter Two
Main Developments in Member States

AUSTRIA

A. New developments and activities

In the reporting period, Parliament passed the **Administrative Jurisdiction Amendment Act 2012**. ([2]) This amendment to the Federal Constitutional Law (B-VG) 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. In the case of the Data Protection Commission, this was not possible in this form, as Article 28 of Directive 95/46/EC stipulates that when the Data Protection Commission is dissolved, a new data protection authority must be established, to which the tasks of the Data Protection Commission will be transferred. A corresponding amendment to the Data Protection Act 2000 (the "DSG Amendment 2014") ([3]) accordingly envisages the creation of a **monocratic Data Protection Authority**, which replaces the Data Protection Commission. An appeal process from the Data Protection Authority to the Federal Administrative Court (itself established in 2014) is also envisaged.

In the reporting period the **"Electronic Health Records Act" (ELGA-G)** was passed. Working document WP 131 of the Article 29 Working Party on the processing of patient data in electronic health records (EHR) of 2007 played a significant role in the creation of the Act, and large parts of it are incorporated. However, the Act envisages a universal opt-out system — partly deviating from the system described in WP 131, which is graduated according to the sensitivity of the data.

For **European Data Protection Day 2012**, 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 new **EU Data Protection Package**. The event took place shortly after the presentation by the European Commission of the drafts of a Data Protection Basic Regulation and a Directive on police and judicial cooperation in criminal matters, and became particularly topical as a result.

In the reporting period, the **ECJ judgment on the independence of the supervisory authority** in Austria ([4]) was also handed down, in which the ECJ ruled against the Republic of Austria on the grounds that the Data Protection Commission lacked independence. It basically found that the office of the Data Protection Commission was too closely integrated with the Federal Chancellery, and expressed misgivings about the position of the managing member (there is at least the appearance of dependence on the Federal Chancellery) and about excessive reporting requirements from the Data Protection Commission to the Federal Chancellor. ([5])

(2) BGBl. I 51/2012 .

(3) BGBl. I No. 83/2013.

(4) ECJ 16.10.2012, case C-614/10, Commission/Austria.

(5) In response to this judgment, the legislature passed the "DSG Amendment 2013", BGBl. I No. 57/2013, which established the Data Protection Commission as a separate authority and staff unit.

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 in 2012. Expenses were covered by the Federal Chancellery budget.
Staff	Till November 2012 20.65 full time posts (16 full-time and 8 part-time employees), from mid November 2012 21.65 posts..
General Activity	
Decisions, opinions, recommendations	149 formal decisions (complaints), 246 Ombudsman cases, 2 recommendations and 61 authorisations (data transfer in third countries, research and surveys).
Notifications	6 197
Prior checks	3 393
Requests from data subjects	Writing: 940 Phone: no written documentation
Complaints from data subjects	Complaints leading to a formal decision: 149 Complaints leading to a clarification or recommendation: 246
Advice requested by parliament or government	This falls within the competence of 2 other institutions: the 'Datenschutzrat' (data protection council) and the legal service of the Government in the Federal Chancellery.
Other relevant general activity information	125 million sector-specific identifiers have been issued, over 5 000 new persons, around 1.1 million new legal persons have been registered in the electronic identities register by the eGovernment register authority which is a part of the Austrian DPA. This authority is in charge and control of the sector-specific identity management used in the Austrian eGovernment.
Inspection Activities	
Inspections, investigations	22, 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

1. Video camera on car

In the reporting year, the registration of a data application "*Video surveillance to protect the monitored object (the position in the immediate vicinity of the user's own private car) or to fulfil legal duties of care, including securing evidence, with exclusive retrieval in the situation defined by the designated purpose, provided that specific facts justify the assumption that the monitored object could be the target or location of a dangerous attack*" was rejected by the Data Protection Commission.

The applicant had applied to enter this data application in the data processing register held by the Data Protection Commission as video surveillance (Sections 50a et seq. DSG 2000). The declarant named the "competent authorities or competent court (for delivering evidence in criminal matters)", "security authorities (for policing purposes)", "courts (for delivering evidence in civil matters)" and "insurance companies (for settling insurance cases)" as the planned recipients of the transmissions. Invited to comment, the applicant stated that the application was meant solely for private purposes (like video cameras on Kärntner Strasse or athletes with helmet cameras), i.e. not for commercial nor non-private purposes. It did not amount to video surveillance in the sense of a systematic, and particularly continuous, recording of events relating to a specific object or a specific person. Where applicable, the recordings could however be used to prosecute criminal acts. There was no specific object to be recorded. Private recordings can be retained for any length of time, and there is no cyclical overwriting of data.

In the grounds for its rejection, the Data Protection Commission stated that the data application in question had to be regarded as video surveillance. It involved a systematic (recording of every journey or at least specific types of journey) and particularly continuous (recording of the entire route) recording of events (road traffic around the vehicle), relating to a specific object (the user's vehicle) or a specific person (at least the driver of the vehicle). This was not an exclusive use of data for personal or family purposes. In this case, monitoring the traffic and the area surrounding one's own vehicle was characterised by the discernible intention to generate evidence for a possible transmission to criminal investigation authorities, courts, etc. This certainly ruled out "exclusive" use for private purposes. Moreover, the applicant did not have the "statutory competence" or "legal authority" to carry out video surveillance in a public place. Based on the state monopoly on the exercise of power, only the security authorities were authorised to carry out video surveillance in public places and their jurisdiction was based on the requirements of the Austrian Security Police Act.

2. In a recommendation, the Data Protection Commission called upon a company not to make acceptance of its General Terms and Conditions (and hence the conclusion of a corresponding contract) dependent on a consent clause included in the General Terms and Conditions.

The intervener stated that the company had used a consent clause in its General Terms and Conditions (T&C) to obtain consent from customers for the use of their data for competitions and fund-raising activities. As a result, the intervener found that his right to confidentiality had been breached, in that he had been obliged by the inclusion of this declaration of consent in the T&Cs to consent to the data applications mentioned in them.

The Data Protection Commission was prompted to instigate proceedings under Section 30 DSG 2000 (Control and ombudsman procedure). The company maintained that this declaration of consent should be

classed as "voluntary" despite being included in the T&Cs, as the offer underlying the declaration of consent represented the voluntary purchase of a product, which the data subject was free to decide upon. Consequently, the declaration of consent connected with purchasing the product was free from compulsion.

The Data Protection Commission (citing various commentaries and also the opinion 15/2011 on the definition of "Consent" within the meaning of the Data Protection Directive 95/46/EU by the Article 29 working party, WP 187) found that, in this case, it was not possible for the customer to conclude the desired contract with the company without also submitting the declaration of consent included in a clause in the T&Cs. The Data Protection Commission found this incompatible with the requirement for voluntary consent as defined in Section 4 no 14 DSG 2000 and Section 8(1) no 2 DSG 2000. Rather, the customer must be given the opportunity to conclude the desired contract without submitting the data protection declaration of consent (the "opt-in" solution), possibly by designing the T&Cs so that the declaration of consent had to be clicked separately.

BELGIUM

A. Summary of the activities and news

From the point of view of legislation, there were four major developments in 2012. The Decree of 13 July 2012 adopted by the Flemish regional parliament on the creation and organisation of a Flemish service integrator (ISF) is the first of them. The ISF is defined as the body that, by virtue of a law (federal or regional), is responsible for organising the electronic exchange of data between different bodies of the Flemish government, and integrated access to the data. Apart from in exceptional circumstances, any communication to and originating from the ISF must be authorised by the Flemish Supervisory Commission (Vlaamse Toezichtcommissie), which was set up in 2010. Federal legislation has also recognised and organised a federal service integrator (FEDICT). Article 7 of the Law in question is particularly important for the running of the Privacy Commission (CPP) as it entrusts the latter with the job of coordinating the award of any authorisations to be issued by various sector committees and indicating which committee is responsible for issuing this authorisation, based on the opinion of the other competent sector committees. The Law of 3 August 2012 on the handling of personal data by the Federal Public Service Finance (FPS Finance) in performing its missions is the result of dialogue between the CPP and this FPS. This dialogue is motivated by the desire of the CPP to see the basic data protection principles sanctified during interdepartmental exchanges and exchanges with other external bodies. A preliminary version of this legislation deviated, to a large extent and in general, from the right to access granted by Article 10 of the Privacy Law (LVP) in the event of an investigation into a taxpayer. Following the CPP's negative opinion on this restriction, the Law was modified and now provides for examination, on a case-by-case basis, of whether or not exercising a right to access would damage an ongoing investigation. Where appropriate, a reasoned, individual decision will be taken regarding restriction of the right to access. Modification of the Code of Journalistic Principles, which now clearly establishes that information taken from social networks such as Facebook cannot be used by the media in their publications without the explicit consent of the individuals in question, is also the result of long dialogue with the CPP. The emotion sparked by the Sierre coach crash in March 2012, following which certain images (mainly of children) taken from social networks were published by the press, most certainly contributed to this. Lastly, the fourth legislative development to be mentioned is the adaptation of legislation relating to electronic communication, transposing into Belgian law the Directive on cookies following a recommendation and an opinion of the CPP. Amongst the other opinions and recommendations adopted by the CPP, we can identify one relating to the introduction of the principle of authentic sources, of a data exchange "crossroads bank" and of a "Wallonia-Brussels" Privacy Commission" for the Wallonia region and and French Community, the counterpart of the aforementioned Flemish Supervisory Commission. In its "Cybersurveillance" Recommendation relating to employer control of the use by employees of electronic communication means in the workplace, specifically email and internet, the CPP offers a fair way of reconciling the required respect for workers' privacy and personal data protection on the one hand and, on the other hand, the respect required for employer prerogatives and smooth running of the company (see also the 2011 report).

European data protection reform

Lastly, the initiative opinion of the CPP on the draft European Regulation filed by the European Commission at the beginning of the year pinpoints the many difficult questions raised and the firm opposition sparked by both the choice of the instrument and the content of this draft reform of the regulatory data protection framework in the European Union in the eyes of the CPP. It substantiates the important work carried out in 2012 to analyse this text.

For further information, all of the CPP's activities are covered in its 2012 Annual Report available at: http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2012.pdf

Organisation	Commission for the protection of privacy
Chair and/or 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 [crossroads bank for social security] 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	€5,684,000 (2012)
Staff	53 employees (1 Chairman – 1 Vice-Chairman) - President's Secretariat (5): legal secretaries (2), secretaries (2), logistics (1) - Administrator (1) - Heads of section: (3) - Personnel and Organisation (16): accounts (1), translators (5), administration (3), statistics (1), personnel manager (1), reception (2), logistics (1), IT support (1), communication manager (1) - Studies and Research (17): legal counsel (15), IT specialist (1), research assistant (1) - External Relations (Front Office) (11): legal counsel (4), assistants (7)
General Activity	
Decisions, opinions, recommendations	- Avis (à la demande du pouvoir législatif ou exécutif - voir ci-après): 41 - Avis et recommandations d'initiative: 9 - Recommandations dans le cadre des déclarations de traitements ultérieurs: 9
Notifications	

Prior checks	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 authorisation requests: - Federal authority sector committee: 46 (individual) and 40 (subscriptions to general authorisations) - Statistics sector committee: 38 (individual) - National Register sector committee: 106 (individual) and 229 (subscriptions to general authorisations) - Social security and healthcare sector committee: consult the Banque Carrefour de la Sécurité Sociale website
Requests 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: 1,892 "Questions & Answers" files opened in 2012 (publicity right, principles of protection of privacy, economy/consumer credit, privacy in the workplace and public authorities). - The CPP also handled 2,896 requests for information or mediation (including inspection files): These files can be broken down as follows: 2,437 requests for information both from public bodies and current or future data controllers and from data subjects, 303 requests for mediation and 156 inspection files.
Complaints from data subjects	See above: 303 requests for mediation: before any mediation or communication of information, the CPP always analyses admissibility. For 149 files, the request for mediation was found to be inadmissible, often due to a lack of information from the data subject (144 files). 198 requests (8.26%) 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. 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) - Privacy and work, credit.
Advice requested by parliament or government	A list of the opinions issued by the Belgian Commission in 2012 is available on its website at: http://www.privacycommission.be

Other relevant general activity information	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	156 inspections. In 2012, the Privacy Commission carried out inspections at 2 levels. The first level involves data processing within the context of, on the one hand, the Schengen, Eurodac and Douane information systems and, on the other hand, Europol activities. The second level concerns initiative inspections carried out. These inspections can be further divided into 3 types: ongoing inspections with Child Focus and the Centre for Information and Opinions on harmful sectarian organisations; themed inspections with the police and information services including files relating to indirect access (covered by Article 13 of the Privacy Law - police sector), and one-off inspections that are always aimed at a specific data controller.
Sanction Activities	
Sanctions	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	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	The CPP does not have this information.

BULGARIA

A. Summary of the activities and news

Organisation	Commission for Personal Data Protection
Chair and/or College	Commission with President: Mrs Veneta Shopova and 4 members: Mr Krassimir Dimitrov, Mr Valentin Enev, Mrs Mariya Mateva and Mr Veselin Tselkov.
Budget	BGN 2 738 678, of which BGN 2 573 917 are spent.
Staff	Number of employed officials: 78
General Activity	
Decisions, opinions, recommendations	In 2012 364 decisions, opinions and instructions were issued in total, of which: - 271 complaints - 77 opinions on the LPPD's application - 16 compulsory instructions
Notifications	66 805 personal data controllers
Prior checks	1 616
Requests from data subjects	247 requests from individuals and legal entities and various inquiries on current issues connected with the CPDP's competences.
Complaints from data subjects	531 complaints — the most were received from the following sectors: - Telecommunications: 274 - Labour and insurance services: 33 - Banks and banking sector: 32
Advice requested by parliament or government	- National Assembly request for opinions on the possibility of making a copy of the provided list with signatures collected under the Act for Direct Participation of Nationals in the State Authority and Local Self-government (ADPNSALS) for prohibiting the research and exploitation of shale gas in Bulgaria by the method of hydraulic fracturing to be submitted to members of the initiative committee and entered in the National Assembly. - Council of Ministers request for an opinion on the creation of a new personal data register and authorisation for access to it.
Other relevant general activity information	With regard to the transfers in the Law for the Protection of Personal Data is foreseen an authorisation regime and during the stated period eight requests were considered for authorisation of third

	countries' personal data transfers. With regard to the binding corporate rules: the CPDP approves lead authority and coordinates the BCR documents under the mutual recognition procedure and in 2012 14 requests for approval were entered.
Inspection Activities	
Inspections, investigations	In 2012 the total number of performed inspections was 1 718 of which: - ex-ante: 1616 - ongoing: 71 - *ex-post*: 32, mostly in the fields of: healthcare: 996; trade and services: 109; education and training: 106; tourism: 58; legal and consultative services: 54 etc.
Sanction Activities	
Sanctions	In 2012, the CPDP's activity on imposing sanctions was as follows: - 58 acts for ascertainment of administrative violations - 52 penalty decrees
Penalties	In 2012, the CPDP imposed sanctions in the amount of BGN 323 350 (appr. EUR 161 675).
DPOs	
Figures on DPOs	N/A

B. Information on case-law

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

In 2012 16 compulsory instructions were issued, most of which were in the public administration field, followed by the financial sector, and then healthcare and the least were issued in the following sectors: judicial power, education and training, transport, trade and services.

The instructions were issued in connection with:

- lack of necessary organisational and technical measures for guaranteeing the personal data protection level: 51 % of the instructions;
- not taking the necessary actions on updating the information, submitted in the CPDP's personal data controllers register: 33 %;
- ban for processing specific personal data categories: 13 %;
- violation of the requirement for receiving informed consent by the individual by the processing of his/her personal data: 3 %.

Among the most common violations of the CPDP for which acts on ascertainment of administrative violation were issued were:

- non-compliance with the requirement for updating the received information in the submitted personal data registers to the CPDP. The violation consists of the processing of a new register, which the controller has not declared in the CPDP and entered in the system;
- lack of instruction for establishing technical and organisation measures for protection of data from incidental or illegal destruction or incidental loss, or unlawful access, rectification or dissemination as well as from other illegal forms of processing;
- non-compliance with the obligation to register in the Commission for Personal Data Protection;
- not undertaking the necessary technical and organisation measures for protection of data from incidental or illegal destruction or incidental loss, or unlawful access, rectification or dissemination as well as from other illegal forms of processing.

2. With regard to issuing opinions on requests and signals — aside from the cases quoted in the table — with which the CPDP was approached by the state authorities, the following opinions are also interesting.

2.1. CPDP's opinions on submitted requests for granting access to the National Population Database

Among the most often submitted requests were those related to the provision of access to the National Population Database maintained by the Directorate-General's Civil Registration and Administrative Services (CRAS) with the Ministry of Regional Development or to the civil status registers.

In the majority of cases data controllers requested the provision of direct access to the National Population Database, which were motivated with the presence of legal interest.

The CPDP's practice on the raised issues related to the direct access to the National Population Database is that a distinction should be made between providing information (data) from the NPD by proven legal interest and granting direct access to the NPD.

The CPDP is of the opinion that there is no legal obstacle for the submission of specific information i.e. personal data (not a direct access) following the legally set procedure in the MRD: DG CRAS in order to exercise the legal interest, when it is proven, of the persons requiring the information.

2.2. Requests for access to public information

The Bulgarian data protection legislation does not regulate issues related to the freedom of information and access to it, which are foreseen in separate law.

Despite that, in 2012, the CPDP also pronounced on requests for opinion from the state and local bodies in connection with access to public information.

Notably the relevant state authorities have received requests for the submission of information about given remuneration in them.

After considering the raised questions, the CPDP issued an opinion that information about specific posts and remuneration falls within the definition of 'personal data' from an economic category identity, only if the individual can be positively identified.

The processing of such information is admissible and legal only in cases when one of the set admissibility conditions is met, such as the existence of public interests or the explicit consent of the individuals.

2.3. With regard to the requests connected with the prevention of conflicts of interest related to the appointment of high-level officials in state administration

In 2012, the Commission for Data Protection gave an opinion, upon request from the Commission for the Prevention and Ascertainment of Conflict of Interest, on whether it is allowed under the LPPD to publish on the Internet — further to a decision by the Commission (for the Prevention of Conflict of Interest) — information related to:

- titles of persons holding public office, in cases where it could be an identification feature of the person;
- the title and the full name of the location where it is carried out, when that location represents an identification feature.

When considering the request for an opinion, the CPDP took into account the fact that the Commission for the Prevention and Ascertainment of Conflict of Interest Prevention has a legally established obligation to publish its decisions on its website under the Law on Prevention and Findings of Conflicts of Interest, thus, the publicity and transparency of the work and the decisions of the Commission is provided, and the authority also has an obligation not to disclose the identity of the person who submitted the signal.

The CPDP expressed the opinion that when the decisions of the Commission for the Prevention and Ascertainment of Conflict of Interest Prevention are published on its website, measures should be taken to ensure the inability for identification of individuals who have submitted a signal, and against whom a signal has been submitted. In this regard besides the initialisation of names and addresses, the features related to physical, physiological, genetic, psychic, psychological, economic, cultural, social or other individuals' identity should be deleted. Following the purpose of the Law on Prevention and Findings of Conflict of Interests and the obligation of persons holding public posts to fulfil their tasks in public interest, honestly, fairly, responsibly and objectively, and to be liable before the citizens and to the authorities, which have chosen or appointed them, the CPDP assumed that in the decisions published on the Commission's website, data for their profession and/or job position, as well as for the location, in which it is exercised, could be published. In the event that the decision contains the personal data of third persons, the latter should be anonymised.

2.4. CPDP opinion on the Direct Participation of Citizens in National Government and the Local Self-government Act

Also interesting was a request for an opinion from the National Assembly on the possibility that a copy of a subscription list under the Act for Direct Participation of Nationals in the State Authority and Local Self-government (ADPNSALS) with a request for prohibiting the exploration and production of shale gas in Bulgaria by the method of hydraulic fracturing, to be provided to a member of the Initiative Committee, which has lodged it to the National Assembly.

The CPDP opinion on that case was that the provision of a copy of the subscription list to a member of the Initiative Committee represents 'personal data processing', which is carried out via the provision of data in accordance with the legal definition referred to in § 1 (1) of the Additional Provisions of the LPPD. Personal data were collected for the national civil initiative, the subscription list was submitted to the National Assembly, as evidence of the copy attached to the obligatory text which indicates that personal data will not be used for purposes other than for the purposes of the Citizens' Initiative for prohibiting the research and exploitation of shale gas in Bulgaria by the method of hydraulic fracturing. The request for the provision of a copy of the subscription list from the National Citizens' Initiative for prohibiting the research and exploitation of shale gas in Bulgaria by the method of hydraulic fracturing prepared under the Act for Direct Participation of Nationals in the State Authority and Local Self-government, to a member of the Initiative Committee represented an additional processing of personal data for purposes other than those for which the data were collected and by means incompatible with those purposes, therefore a copy of the subscription list should not be submitted.

C. Other important information

1. The Commission for Personal Data Protection adopted a new Ordinance for the minimal level of technical and organisation measures and admissible types of personal data protection

On 30 January 2013, the Commission for Personal Data Protection adopted a new Ordinance on the minimum level of technical and organisational measures and the admissible types of personal data protection. The Ordinance was issued on the ground of Article 23 (5) of the Law for Protection of Personal Data. It was published in the State Gazette on 12 February 2013 and entered into force three days after its promulgation. This Ordinance repeals Ordinance No 1 of 7 February 2007.

The Ordinance aims at ensuring adequate personal data protection depending on the data nature and the number of individuals concerned, in case of violation of the data protection. The Ordinance defines the main personal data protection purposes: confidentiality, integrity and availability. It introduces five different types of personal data protection: physical protection, personal protection, documentary protection, protection of automatic information systems and/or networks and cryptographic protection. Furthermore, the Ordinance introduced the 'need to know' principle as to the access control.

In order to determine the adequate level of technical and organisational measures and the admissible type of protection, the controllers are obliged to periodically carry out an impact assessment on the processed personal data. The impact assessment aims at determining the different risk degrees and the corresponding levels of protection. Each level of protection corresponds to a precise combination of technical and organisational measures to be undertaken by the data controllers.

The new rules provide for four levels of impact, depending on the extent of the adverse effects that may be caused by unauthorised processing of personal data: 'extremely high', "high', 'average' and 'low'.

Since the Ordinance came into force, the Commission started trainings and consultations of data controllers in order to raise awareness of the new issues concerning personal data.

The Ordinance is available in English on the website of the CPDP.

In general, the Commission for Personal Data Protection places emphasis on trainings of personal data controllers in accordance with the adopted Annual Training Plan. Furthermore, experts of the Commission for Personal Data Protection are invited by the Institute of Public Administration (the national training centre for civil servants) to conduct regular training courses in the data protection field, starting from October 2013.

2. Practice under Directive 2006/24/EC on data retention

Directive 2006/24/EC of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) was transposed into the Bulgarian legislation via amendments to the Law on Electronic Communications in 2010. After analysis of the statistical information provided in 2012 by the enterprises providing electronic communications networks and/or services, the Commission for Personal Data Protection analysed the problems and trends in the process of traffic data retention at a national level. The Commission found the following areas of concern:

- Legal grounds, for which access to traffic data may be requested, does not correspond to entities empowered to submit these requests and the range of bodies foreseen in the LEC as competent to request references, but is wider than that which actually has the right to do that (the National Intelligence Service is among the authorities mandated to request access, but does not have the competence to disclose and investigate serious crimes).

- Classification of the requests for access and the disposition of the court lead to the inability for the provision of reference by Internet service providers which do not have a registry for classified information;
- Companies providing electronic communications networks and/or services express their concerns that control on requests for access from investigating police is missing and that the category of persons uses an extremely easy way to obtain traffic data references. The Prosecution Office of the Republic of Bulgaria supports the approach that the request for access for the needs of pre-trial proceedings is to be submitted by an investigating body with an explicit written authorisation from the monitoring prosecutor.
- There is a trend for reducing the number of enterprises that have fulfilled their legal obligation to provide statistical information (for comparison, in 2011, 33 enterprises provided statistical data, and in 2012, 22 enterprises). It is evident, however, that large enterprises in this market provide accurate information from which to large extend can be outlined the trends and which is also a strong basis for statistical analysis.
- Despite the CPDP position that the requirement of the LEC for submission of information on 'cases under which data have been provided to the competent authorities' involve the provision of a specific and detailed statistics on all separate cases, the enterprises are not able to submit such information, and therefore provide only summary data on the total number of cases for access requests.
- There is an almost double increase in the cases in which the competent authorities have asked for traffic data provision (for comparison, in 2011, requests for access to retained traffic data were 39 781, and in 2012, 75 672).
- The number of cases in which data has been provided to the competent authorities under LEC almost doubled (for comparison, in 2011, total of 38 861 were provided, and in 2012, 74 296); the number of cases in which no response to the request for data could be given has also increased (for comparison, in 2011, there were 920, and in 2012, 1 376).
- Statistical information received by the CPDP from the enterprises is summarised and based on different criteria and parameters, and does not fully comply with the types of information that the European Commission expects to receive.

In order to meet the expectations of the European Commission and to take measures for unification of the practice at national level, the Commission for Personal Data Protection issued mandatory instructions to the entities liable under the LEC.

The mandatory instructions regulated all parameters discussed at the meetings held with the institutions involved in the data retention process.

The instructions specify the requirements on the content of the registers maintained by the authorities under Article 250(b) of the LEC, the courts and the enterprises providing publicly available electronic communications networks and/or services, as it is explicitly stated that these requirements represent the minimum required content. Any of the liable persons may also, at their own discretion, require the entry of additional information in the registers. It is indicated that the registration, storage and destruction of documents related to the requests for access, permits issued and refusals, orders for access and references, are determined by internal rules of the authority under Article 250(b) (1) from the LEC, a court or enterprise, for working with opened and classified documents subject to the applicable legal acts. The requirements for destruction of stored data are drawn up.

CYPRUS

A. Summary of activities and news

The Commissioner's Office was actively involved in the discussions for the data protection Package of Proposals presented by the Commission in January 2012. In February 2012 a Memorandum of Understanding was concluded between the Commissioner and the Minister of Justice of Public Order, establishing a procedure for the adoption of common positions and appointing a DPA Officer to chair DAPIX, the Council Working Party in which the package of proposals was discussed. In March 2012 the Commissioner's Office, in association with the Ministry, launched a public consultation for these proposals and had numerous meetings with major stakeholders, before and during the CY Presidency. The CY chairing of DAPIX, advanced the proposals' discussions and identified a number of horizontal issues for which delegations shared common concerns, namely the large number of delegated and implemented acts embedded in the proposals, the administrative burdens for small-medium enterprises and unclear rules/derogations for the public sector, which were discussed in the Friends of Presidency informal meetings. The work carried by the CY Presidency is reported in the relevant Progress Report adopted by the JHA Ministers' Council in December 2012.

In the frame of activities for celebrating European Data Protection Day, the Commissioner's Office used a budget of EUR 4,300 for disseminating, on 28 January, printed information material and gifts (alarm clocks and light torches) with the Office's logo and e-mail address. The message of the day was *time for awakening, time for enlightenment*. A number of TV and radio appearances were made by the Commissioner and his Officers.

In 2012 the basic Law (Law 138(I)/2001) was amended with the aim of better transposing the provisions of Directive 95/46/EC, in line with the Commission's comments in the frame of a structured dialogue and to improve the effective functioning of the Commissioner's Office.

In 2012 the Commissioner's Office examined a complaint against an insurance company, which allegedly requested from the complainant a disproportionate number of medical documents to support her compensation claim for inability to work due to her health condition. Having examined the insurance contract's terms and the number of (additional) documents that the complainant had at times been requested to submit, the Commissioner asked the company to justify why it had not, at some point, either accepted or rejected the claim, taking into account a proportional number of documents but, instead, prolonged the claim's examination by asking for additional tests and documents, a practice that, at first sight, seems to be in breach of the proportionality principle. The case is still under examination, pending the Commissioner's Decision.

Pursuant to the examination of a complaint filed by employees, through their Unions, against two private hospitals that recently installed systems for monitoring work attendance, making use of biometric data (fingerprints) stored only on smart cards issued to employees, not stored in a central database, a Decision was issued concluding that the use of these systems was in breach of the proportionality principle. The hospitals were called to cease processing and uninstall the systems. While one hospital complied the other did not and challenged the Decision before the Court. The ruling is pending.

Organisation	Office of the Commissioner for Personal Data Protection
Chair and/or College	Mr Yiannos Danielides
Budget	Allocated budget: **EUR** 307 570 Executed budget: **EUR** 265 609
Staff	Administrative Officers: 7 Information Technology Officers: 2 Secretarial officers: 6 Auxiliary staff: 2
General Activity	
Decisions, opinions, recommendations	Opinions: 47 Decisions: 5 Recommendations: 1
Notifications	260
Prior checks	N/A
Requests from data subjects	In writing or by phone: N/A
Complaints from data subjects	Licences for combination of filing systems: 43 Licences for transmissions to third countries: 46
Advice requested by parliament or government	In 28 occasions our Office was invited to Parliamentary Committees of the House of Representatives for advice/ consultations
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	Number of Audits: 1. Number of investigated complaints: 233 out of 325
Sanction Activities	
Sanctions	In one Decision the Commissioner the administrative sanction of cessation of processing and destruction of the personal data. In another Decision, the Commissioner issued recommendations to the controller.
Penalties	In 3 Decisions fines were imposed to controllers that total **EUR** 3 500
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In 2011, the Commissioner, in accordance with Section 23(a) of the Law, reported to the Chief of the Police a possible criminal offence committed by a journalistic website for not complying with the Commissioner's Decision to cease processing and destroy asylum seekers' personal data that had been published in breach of the proportionality principle, in an article uploaded on the website for weeks, and for not paying the EUR 3 000 imposed on it. The case was brought before the Court. Since the defendant informed the Court of its subsequent compliance to the destruction of data and ceasing of processing, the Court ruled in favour of the Commissioner's decision and called the website to pay the fine as a civil debt.

CZECH REPUBLIC

A. Summary of activities and news

We received a **grant** from the Leonardo da Vinci Partnership programme for an international project, Raising awareness of data protection issues among employees working in the EU. The aim was to prepare a comprehensive handbook destined for a broad audience of European employees and to organise accompanying events to improve public awareness. The project partners are DPAs from Poland (project coordinator), CZ, Bulgaria and Croatia. The project shall end in July 2014.

On 12-14 March 2012 we hosted at our office a **three-day study visit** for three members of the Albanian DPA. The event was funded by TAIEX and focused on complaint handling, investigation procedures, registration and activities or press departments.

On 11-12 June 2012, one of our experts attended as speaker the **TAIEX seminar** on inspections and data protection compliance organised by the Macedonian DPA in Skopje.

On Data Protection Day we launched the sixth edition of the **children and youth competition** 'My privacy! Don´t look, don´t poke about!' designed to promote privacy awareness among the young generation. This time we concentrated on Internet use and encouraged competitors to think about privacy consequences by submitting an essay, narrative, video clip or comic strip. We received 67 contributions, three of them were awarded.

Organisation	Office for Personal Data Protection - Czech Republic
Chair and/or College	Dr Igor Němec, President
Budget	CZK 146 219 000 = EUR 5 665 207 (exchange rate as of August 2013 — 25.81 CZK/EUR)
Staff	97 permanent staff (out of which about 10 are from facility management and accounting, i.e. not directly connected with data protection).
General Activity	
Decisions, opinions, recommendations	12 opinions (prevailing topics: video surveillance, Internet, marketing). An in-depth methodology for controllers operating video surveillance systems published (available also in English).
Notifications	5 169 notifications (out of which 4 618 registered). The number of notifying controllers is 3 397 as some of them notified more than one processing operation.
Prior checks	105
Requests from data subjects	2 503 (out of which 47 from foreign subjects). Consultation was sought not only by individual data subjects, but also by legal persons and public authorities.
Complaints from data subjects	Complaints - 1319 (out of which 197 submitted for further

	inspection, 69 submitted for administrative proceeding, 13 forwarded to other public administration bodies, 1 040 declined as unjustified). Beside this, 7 933 complaints received concerning spam (out of which 3 772 accomplished).
Advice requested by parliament or government	The parliament requested advice on two occasions: on PNR and on the draft DP regulation.
Other relevant general activity information	Involved in the **inter-ministerial comments procedure**, we assessed and commented on 85 bills and 94 draft implementing regulations.
Inspection Activities	
Inspections, investigations	129 inspections (investigations) initiated, 9 accomplished (but started the previous year). This figure does not include actions related to spam. In this area, 87 inspections were initiated and also accomplished (plus an extra one started the previous year).
Sanction Activities	
Sanctions	49 sanctions. Additionally, in the area of spam, we imposed 3 sanctions. Explanatory note: Under sanctions, 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 sake of information value a set of sanctions under a particular investigation is counted as one. The average for one action is about 2.7.
Penalties	125 penalties; apart of this 23 penalties were imposed for spam.
DPOs	
Figures on DPOs	Not applicable. DPOs not anchored in the Czech DP law.

B. Information on case-law

We launched, on the basis of a request, an **inspection at the Czech Post**. The deliverers were carrying a GPS device to monitor their whereabouts. Czech Post said it had introduced the system to be able to handle complaints from clients who said delivery staff failed to deliver a parcel/registered letter. We ruled that the processing of personal data (monitoring of field employees) had no legal ground so that Czech Post had breached the Data Protection Law. The Czech Post objected this finding in 2012. The case was therefore forwarded to an administrative proceeding.

We conducted an **inspection at a pharmacy retail chain** based on a client´s complaint concerning use of personal data stored on the client card. The inspector suspected breach of the Data Protection Act, more precisely of two Articles related to the liquidation of data and the data subject´s rights respectively. The company also processed sensitive client data. The official purpose of the processing was maintenance of client medicinal records in order to detect contraindication, interaction of medicines prescribed, or allergies. All data were collected with the data subject´s written consent. The inspection revealed that the company

has sufficient technical and organisational measures in place. However, they failed to immediately destroy data on the client´s request, or after the client card had been cancelled. The reason was insufficient staff training. The shortcoming was removed immediately during the inspection. Therefore, no sanction or penalty was imposed.

A **double-track inspection was conducted at a Prague hospital**. The first leg of the inspection was initiated by the annual inspection plan and focused on marking patients with identification bracelets. The other was based on a complaint pointing that a video from an operation was posted online together with a patient´s personal data (name, partial surname, birth date) enabling his/her identification. As for the bracelets, they are handed over to every patient upon reception. They are either blue for standard patients or yellow for patients with serious diagnoses. The bracelets contain different data as to the identification, diagnosis and treatment, etc. The bar code on these bracelets is readable from only 10-20 cm which prevents any possibility of monitoring the patient´s whereabouts in the hospital area. In the case of the online video, the hospital management presented a form, containing an informed consent by the patient in question. They said moreover, that disclosing the birth date of the patient was not their primary purpose in the process and removed the entire footage from the Internet. The Office´s inspector thus concluded that in neither case had the Data Protection Act been violated.

Another sample inspection was conducted at a **housing association** which posted an online (and freely accessible) list of their members-debtors, featuring name, surname and the amount of the debt. The association is authorised to keep evidence of debts without the debtors´ consent as follows from the relevant provision of Data Protection Act reading that personal data may be processed if it is necessary for the protection of the rights and legal interests of the controller. The other way round, such processing must not be at variance with the data subject´s right to the protection of his/her private life. The processing in question would not be in contradiction with this data subject´s right, if accessed merely by the association members, who are the creditors. The debtors´ consent would be needed for unrestricted disclosure online. Therefore, by publishing the list of debtors along with the size of their debts on the association´s website accessible for everyone, the housing association had breached the Data Protection Act. The Office fined the association a financial penalty. The controller has taken a remedial measure by making the relevant webpage password-protected.

Further interesting cases are thoroughly described in the Czech DPA´s annual report. English version available at: http://www.uoou.cz/uoou.aspx?menu=159&lang=en .

C. Other important information

We entered the year 2012 equipped with a new competence as to the **data breach notifications** in the area of e-communications. To this end, we have started a special section on the Office´s website featuring the list of relevant regulations, an explanation of obligations and notification forms (one for breach notifications of the Office, another for notifications of the data subjects concerned). Altogether we received only one notification in the reference period (in 2013, we have also received one notification so far).

The inspectors conducted inspections at three Czech Republic **embassies and consulates** (Russia, Turkey and Kazakhstan). They focused namely on the processing of personal data in the course of visa proceedings and within the Schengen Information System. The physical security of databases was checked out too.

We received 18 applications for **international data transfers**, none of them was refused, 13 were approved, five were suspended due to procedural reasons.

DENMARK

A. Summary of activities and news

Organisation	Danish Data Protection Agency
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 (approx. 15 cases per year) are put before the Council for a decision. The Council is chaired by a Supreme Court Judge.
Budget	DKK 21.1 million.
Staff	Approx. 35
General Activity	
Decisions, opinions, recommendations	N/A (included in the figures below)
Notifications	2 031
Prior checks	2 031
Requests from data subjects	2 062 This number covers all requests and complaints made to the Danish DPA)
Complaints from data subjects	See above
Advice requested by parliament or government	444
Other relevant general activity information	26 cases relating to security
Inspection Activities	
Inspections, investigations	58
Sanction Activities	
Sanctions	Each year the Danish DPA expresses criticism to several data controllers for not complying with the Act on Processing of Personal Data.
Penalties	Fines in six cases.

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

B. Information on case-law

Live transmission from church services

A church in the city of Ribe contacted the Danish DPA with an enquiry regarding the compliance of the Danish Act on Processing Personal Data and a live transmission from a church service. The purpose of the transmission was to give people, who by various reasons were hindered from participation, an opportunity to observe the ceremony. A sign at the entrance of the church clearly described the video recording taking place in the church.

The Danish DPA assumed that the church congregation was responsible for the processing of the personal data in that situation. It was then up to the congregation to make the relevant balancing of the legitimate interests of the transmission, and the interests of those being filmed.

To this end, it was also notable that the church service was open to the public, and the receivers of the transmission were a specific and limited group of people, like the elderly at a retirement home.

The initial assessment of the Danish DPA was that the Danish Act on Processing Personal Data does not prohibit the transmitting of specific church services, as long as the participants are clearly informed, and that the transmission was controlled to be directed to specific locations. In some situations — such as a baptism — the written consent of the participants is still needed.

C. Other important information

Video surveillance conducted by housing organisations

In 2012, the Danish DPA initiated a series of inspections especially aimed towards video surveillance in private housing organisations. The purpose of the project was to gather practical experience in this particular field and build up awareness in relation to data protection conducted by private companies and natural persons. The most common issues were extensive data retention and filming interfering with the private sphere of some apartments, but a decent respect of private life and data protection was shown in general.

The experiences gathered from the project were accumulated in a comprehensive set of guidelines, published both in print and online.

International data protection day

The Danish DPA spent International Data Protection day with an in-house arrangement trying to educate and inform the general public about data protection. The staff arranged tours around the office premises, gave presentations and had an open Q&A session for the participants. The day was a success for both staff and visitors who showed a great knowledge and interest in personal data protection.

BCR

Denmark received a numerous number of BCR applications, which means that Denmark is going to be lead authority on a few occasions.

An increased number of Danish companies have realised the opportunities of the BCR-model, because the model means greater flexibility regarding transferring data to third countries, as soon as the rules are prepared and implemented. As this trend continues, the Danish DPA expects the number of applications to increase in the future.

2012 was also the year where the Danish DPA was BCR 'co-reader' in a BCR process with the British ICO as lead authority.

ESTONIA

A: Summary of the activity and news:

The main task of the Data Protection Inspectorate is to ensure that:

- a person's right to privacy is respected when personal data are used,;
- public information is accessible.

The Inspectorate is therefore the implementing agency and independent regulator of the Personal Data Protection Act and the Public Information Act.

The legislator has also assigned various other tasks to the Inspectorate. We have also been assigned tasks with international legislation ([6]).

As the protector of information-related fundamental rights the Inspectorate performs the role of an independent commissioner that resolves complaints and investigates breaches at its own initiative. The number of inquiries and cases of supervision has stabilised in recent years:

	2012	2011	2010
Received memoranda and requests for explanation/information	877	940	893
Help line calls	1202	816	1061
Initiated supervision proceedings [2]	595	481	588
Misdemeanor procedures (completed)	43	34	35

Use of personal data can be highlighted as a common subject in inquiries and proceedings:

a) in employment relationships (e.g. monitoring employees, suitability of a consent or contract for data processing, continuing the use of an e-mail address in the name of a former employee);

b) disclosure of debt data (primarily disclosure without the filter of legitimate interest, disclosure of the members of managing bodies of indebted legal entities);

c) in social and online media (in simple terms, this may be described as a person's request to have their name deleted from Internet search engines, mostly related to social media);

d) electronic direct marketing (unwanted advertisements sent by e-mail and text message).

The use of cameras to monitor people and also the publication of recordings in social media, companies and educational institutions is a growing concern.

In the legal sense, the focus of questions and disputes is usually on the legal basis of data processing — whether or not the person's consent for data processing was obtained, whether or not a contract or legal act could have been the legal basis for processing without consent.

([6]) The legislator has assigned additional tasks to the Inspectorate with the **Electronic Communications Act** (supervision of electronic direct marketing also in case it does not concern personal data; processing the breach notifications of communications undertakings whilst permitting not to inform the data subjects, separate elements of misdemeanour), the **Official Statistics Act** (participation in the work of the Statistics Council, separate elements of misdemeanour), the **Act on Implementation of Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative** (certifying the compliance of online systems for collection of statements of support), the **Digital Signature Act** (suspension of the use of certificates in case of suspicion), the **Human Genes Research Act** (approval of the method for generating codes for data), the **Population Register Act** (expressing an opinion on the appointment of the authorised processor of the register, approving the contract for maintaining the register, granting permission for exceptional data processing contracts), the **Environmental Register Act** (expressing an opinion on the appointment of the authorised processor of the register, granting permission for cross-usage of personal data). Some tasks arise **directly from international legislation**, especially those that concern participation in the joint supervision of cross-border information systems (the Schengen information system, the Europol information system, the European visa information system, the customs information system and the Eurodac fingerprint register).

There are fewer cases that concern public information - they comprise 10 % of requests for explanation, 18 % of calls to the information hotline and a quarter of complaints and challenges.

Establishing access restrictions remains the most common topic in the area of public information: such restrictions may be excessive as well as inadequate (access to documents that infringe on privacy via online document registers).

However, the most complicated legal disputes arise over the issue of whether or not a person in private law is someone who performs public tasks and is therefore also a possessor of public information.

Misuse of the Population Register is the most common reason of misdemeanour proceedings (30 of 43 completed proceedings). Misuse of the police database has decreased (4 misdemeanour cases).

Our primary goal is to end breaches, not to punish. The majority of breaches end immediately when supervision starts or when a recommendation/proposal is received. In 2012 we issued precepts in just 48 cases ([7]). We imposed coercive and misdemeanour fines in 39 cases.

Organisation	Estonian Data Protection Inspectorate
Chair and/or College	Director General
Budget	EUR 595 403
Staff	18
General Activity	
Decisions, opinions, recommendations	582
Notifications	608 registrations of processing of sensitive personal data
Prior checks	23
Requests from data subjects	877
Complaints from data subjects	404
Advice requested by parliament or government	21
Other relevant general activity information — opinions on public sector information systems	84
Inspection Activities	
Inspections, investigations	457

([7]) This figure does not include standard precepts for guaranteeing the obligation to register controllers of sensitive personal data processing — there were 130 such cases in 2012.

Sanction Activities	
Sanctions	40 cases
Penalties	EUR 5 918
DPOs	
Figures on DPOs	137

B. Information on case-law

The number of proceedings concerning the misuse of health data increased in 2012. The reason for this is simple — we established cooperation with the Health Board and the e-Health Foundation. We exchange information about possible breaches. We carried out two audits in the health sector and found that the organisation of personal data protection in the State Agency of Medicines and the Health Insurance Fund complies with requirements.

In the area of supervision of database maintenance we also carried out personal data protection audits in Viljandi County Government, the Rescue Board and Narva City Government. Supervision in the latter two is continuing due to the omissions we identified.

In the interests of legitimate data processing we checked the logs in the register of self-restrictions of gamblers (the Tax and Customs Board, omissions were eliminated and supervision was ended), in the payroll software of state agencies (the Ministry of Finance, follow-up inspection will continue in 2013) and in the database of the Estonian Traffic Insurance Fund (follow-up inspection will continue in 2013).

Concertation using the detailed descriptions uploaded in the administration system of the state's information system also helps to identify problems in the area of database maintenance. The Inspectorate is one of the coordinating agencies that monitors compliance with personal data protection and public information requirements. The number of concertation proceedings was 84 in 2012 (including 16 refusals) and 81 in 2011.

Comparative monitoring of the disclosure of debt data of natural persons in November 2012 covered the websites of 66 debt collection companies. 12 of them had disclosed the names and often also the dates of birth or personal identification codes of private persons on public websites. Seven of these companies terminated the breaches voluntarily, five did it after we had issued them with precepts.

C. Other important information

Reviewing requests for explanation and complaints is a reaction aimed at individuals and individual questions. It basically means dealing with the trees, not the forest.

We must use the little resources we have left after reacting to problems in the most effective manner: for the prevention of problems, giving information, preparation guidelines, advising important initiatives and development of cooperation.

Preparing the opening of the electricity market is an example of prevention — the Inspectorate participated in the steering group of the electricity market data warehouse for a year as an adviser on issues concerning protection of the privacy of clients. Only one actual incident later occurred in this area ([8]).

([8]) One of the electricity sellers, 220 Energia OÜ, made it possible to access the data of consumers on the basis of personal identification codes. There was an attempt to misuse access, but it was immediately detected and access was made possible only with ID cards.

Our first priority in the protection of personal data in 2012 was protection of the privacy of minors. We dedicated our annual conference (held on 27 January) to this topic. The Guidelines of the Chancellor of Justice on Informing about Children in Need of Assistance were also introduced at the conference. We joined the cooperation project *Targalt Internetis* (Be Smart Online) that is led by the Estonian Union for Child Welfare — we would not be able to reach such a large audience if we acted on our own. We aimed the online game *Päästa Liisa ID* (Save Liisa's ID) at teenagers. We continued giving information on the user account opened for the game in social media. We spoke to teachers of social studies at the seminar organised by the Estonian Atlantic Treaty Association (on 26 October).

Cooperation with the Labour Inspectorate in 2012 was the continuation of the 2011 guidelines on personal data protection in employment relationships. We took part in the four regional lecture series of the Labour Inspectorate and explained the subject of personal data of employees to employers, human resources specialists and trade unions. The Labour Inspectorate also published our guidelines in both Estonian and Russian. We are very grateful to our colleagues from the Labour Inspectorate for this great cooperation.

Estonia became a member of the Schengen Convention in 2007. The abolishment of border control on internal borders is compensated for with information exchange between the law enforcement authorities of Member States via the Schengen information system and the visa information system. The risk that information systems may be misused is managed with strict data protection rules. Once every five years the Member States all evaluate each other to check whether the activities of their authorities comply with the Schengen requirements. Evaluation committees consisting of the representatives of data protection authorities check adherence to data protection rules. This includes evaluating the day-to-day work and supervision carried out by the police, border guards and consular services in the area of data protection as well as the general capacity and independence of data protection authorities.

The Inspectorate participated in the evaluation of six foreign authorities in 2011 and 2012. The Baltic States were evaluated in October 2012. Estonia needed a follow-up evaluation in the area of data protection in 2007, but this time we passed the evaluation without any observations.

The evaluation committee found our online Schengen information (thorough and harmonised information in three languages on the websites of the Inspectorate as well as associated authorities), the regular cooperation between Estonian authorities and the cross-border activities of Baltic data protection authorities to be exemplary.

We would like to acknowledge the contribution made by our colleagues in the Police and Border Guard Board, the Ministry of the Interior, the Ministry of Foreign Affairs and the Information Technology and Development Centre of the Ministry of the Interior to the achievement of positive results in the evaluation.

Detailed guidelines aimed at the senders and recipients of e-advertisements were completed on 22 February 2012 in the area of electronic direct marketing. The draft of these guidelines was discussed in the public advisory committee of the Inspectorate as well as with business organisations and the Consumer Protection Board. The guidelines were introduced in the *Äripäev* business newspaper on 15 March 2012. We also constantly refer to the guidelines in the course of proceedings and in correspondence.

Scientific research permits were our broadest activity in the area of research and statistics. In 2012 we issued 13 permits and refused to issue them in three cases. We also carried out random follow-up inspections of data security in the research institutions to which we had granted permits. In 2012 we inspected the Tallinn University Institute of Demography, no omissions were found.

We also observed the Population and Housing Census during the first three months of 2012. Our colleagues from the Estonian Information System Authority helped us with advice. Statistics Estonia quickly eliminated the small omissions found in the online census, and no big problems were found. As far

as we know, participation in the Estonian online census achieved a world record: 62 % of all enumerated people.

In international cooperation the Inspectorate participated in the activities of numerous workgroups.

Cooperation between Baltic data protection inspectorates was successful from the practical point of view - our Lithuanian colleagues joined the partnership of Estonian and Latvian authorities in 2012. We carried out a joint audit in all hotels operating under the Radisson Blue brand. The audit covered the processing of the personal data of clients and staff members.

We will continue with joint supervision activities also in 2013, when our focus will be on the gambling sector.

The data protection reform plan of the European Union was the most significant international topic. The opinion expressed by European data protection authorities on the reform plan in the opinion adopted on 23 March 2012 was generally positive, but also contained a number of observations and criticism. The opinion was not unanimous, as many data protection authorities did not support it for various reasons.

Updating broader international documents has also been discussed in association with the data protection reform plan of the European Union. The Inspectorate participates in the advisory committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of the Council of Europe. The negotiations of experts for the amendment of the Convention of 1981 ended in 2012.

We also represent Estonia in the data security and privacy protection workgroup of the Organisation for Economic Co-operation and Development (OECD) with the Ministry of Economic Affairs and Communications. The workgroup discusses the amendments to be made to the central privacy document of the OECD — Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The discussion is ongoing.

FINLAND

A. Summary of activity and news

The Commission's proposal includes, for instance, a proposal on a so-called consistency mechanism, meaning a legal instrument aiming — like the entire reform — at better harmonisation of data protection and creation of a genuine EU digital single market. In such cross-border data protection issues, the decision-making would take place in a new EU Data Protection Board to be established. However, since most of such cross-border issues already seem to be 'local' Nordic issues, we have already practised using the instrument with our Nordic colleagues.

In November 2011, Finland was faced by a barrage of hackers. Did we learn anything about these security breaches? We tried to answer this question during the year under review by conducting an extensive survey of the parties that had been attacked by hackers. We aimed at finding out what kind of problems the security breaches caused and what kind of measures the organisations took to correct the situation. The final results of the survey were fairly gloomy: most of the respondents withdrew from the digital market as a result of the security breach. A very common response was for the controller to do nothing!

When preparing for the above-mentioned survey, we arranged an extensive workshop on data security as part of the 25th anniversary of our office. During this workshop, the guests — consisting of top competence in the sector — were posed two questions: is there any need to improve data security in Finland and if so, is the competence needed to do so available? Unfortunately, the guests' reply to the first question was affirmative and to the second negative. Perhaps the data account guide we published will assist organisations in utilising their modern accounting capabilities.

In addition to the above-mentioned workshop, workshops on telephone directory business, social media (whether there are 'grey areas' that the authorities cannot govern in social media), voluntary operational control and data protection for entrepreneurs were arranged during the year under review. The anniversary year culminated in a seminar called KnowRight2012 arranged in Finland, in which we were one of the arranging parties.

As the Council of Europe was drafting a recommendation on profiling, we published a sector survey on regular customer systems that was implemented early in the year ([9]). We found out that the legal quality of regular customer systems varies to some extent. Some of the respondents could not say why they use a regular customer system.

Organisation	Office of the Data Protection Ombudsman
Chair and/or College	Reijo Aarnio has been the Data Protection Ombudsman since 1 November 1997.
Budget	The overall annual budget is EUR 1 737 000.
Staff	The total number of staff is 20.
General Activity	
Decisions, opinions, recommendations	2 946

([9]) Sector survey is a tool we have developed. Its goal is as efficient inspection activities as possible utilising technological means.

Notifications	427
Prior checks	see notifications
Requests from data subjects	986
Complaints from data subjects	(access and rectifications) 180
Advice requested by parliament or government	122
Other relevant general activity information	Cooperation work with data controllers in the following sectors: Education, Health Care, Social Affairs, Telecommunications, Employment and Economy, Marketing
Inspection Activities	
Inspections, investigations	102
Sanction Activities	97
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	> 1 000

B. Information on case-law

At the request of the Data Protection Ombudsman, the Data Protection Board commented the strong identification system required in some booking systems. The case referred to the legal quality of an online service of an optician store chain where people booked appointments and implemented other actions using their name and social security code. The Board agreed with the Ombudsman's statement that the system in question is not secure enough and social security codes are being used to separate people from each other in databases. The controller in question has started to repair the system.

At the request of the Data Protection Ombudsman, the Data Protection Board studied CCTV monitoring in the stairwells of residential buildings as an important matter of principle. The case referred, among other things, to the link between the Personal Data Act and the Criminal Code of Finland. The Board stated as its opinion that CCTV monitoring is possible also in these facilities based on the stipulations of the Personal Data Act.

C. Other important information

Partly due to the lack of comprehensive legal praxis, the Ministry of Transport and Communications ordered a survey on the legislative status of digital estates from Professor in Inheritance Law Urpo Kangas of the University of Helsinki. One of the conclusions of the report was that more specific legal regulations should be made.

The Data Protection Ombudsman assisted the consumer protection authority in determining policies on the legal nature of services based on geographical information that are funded by means of advertisements. In this case, the key question was the link between contractual terms and consent.

Plenty of interesting developments

A continued legislation project during the year under review was the compilation of 'an information society code'. Our office also participated in the work of the steering group and specific sub-groups, whenever possible. In my opinion, parties acting in the digital economy and service production have difficulties in finding legislation to guide their operations, mainly due to the fragmented nature of the legislation ([10]). This is one of the reasons why parties active in the sector may be unsure and uncertain, which in turn may hamper development.

One important reform that received fairly little attention was the implementation of employee tax numbers. In Finland, each person is issued with a social security code (HETU) that is entered in the Population Register and an electronic ID to be used when dealing with the authorities (SATU). Furthermore, the Tax Administration has now implemented a tax number issued to all employees in an attempt to curb the grey market. At least in this respect, the public administration seems to manage the risks pertaining to the management of identities. On the other hand, the development of mobile services based on SATU has had a fairly slow start.

Another step forwards by the public administration is the development regulated by the Act on Public Data Administration that entered into force in 2011: the control on the utilisation of information technology has been further centralised to the decision-makers of state-owned enterprises. One of the proposals issued over the course of the year was establishing an IT service company owned by the State. The national auditing based on the Data Security Decree seems to have started well.

Data balance sheet

The Office of the Data Protection Ombudsman has on 24 April 2012 released a guide called Prepare a data balance sheet. The data balance sheet is a knowledge management report based on an internal review, which aims to help organisations assess their data processing practices. It may also be used to report key data processing issues to the organisation's stakeholders. The data balance sheet is intended as a dynamic tool, which supports the efficiency, impact and competitiveness of the organisation.

While the data balance sheet may supplement statutory reporting based on financial statements and annual reviews, the purpose is not to unduly add to the administrative burden of the organisation. The data balance sheet also complies with the principle of accountability, according to which an organisation itself demonstrates its compliance with legislation and good practice in data processing and information management. In the future, data protection legislation may require the introduction of practices complying with the accountability principle.

The purpose of the guide is not to present an exhaustive formula or list of the information to be included in the data balance sheet. Its contents may vary, depending on the sector in which the organisation operates and the nature of its operations. Therefore, it is advisable to introduce the data balance sheet to the extent to which it is expected to have a positive impact on the organisation's operations.

The Office of the Data Protection Ombudsman participated in the control of the above-mentioned issues and the control of scientific research, supervision of DNA sample collections, issues pertaining to intelligent transportation systems and road tolls, communication on threatening data leaks from smart phones, reform of the Act on Processing Personal Data by the Police, the work of the Human Rights Committee and many other projects. In addition to these intensive daily tasks — of which there is further

([10]) An example of this is a Government Bill on regulating the use of biometrics in the Radiation Safety Act that was being processed by the Parliament. There is no specific Finnish act on biometrics.

information in other sections of this annual report - we need to look at issues from a broader perspective. Part of this broader perspective comes from the currently ongoing extensive European and Nordic cooperation ([11]) while part comes from participation in NETSO, a project funded by the Academy of Finland and led by Professor Ahti Saarenpää, that horizontally studies the development of the information society.

([11]) As part of the Nordic cooperation, we implemented an extensive review of Facebook with our Norwegian colleagues. The review started in 2011.

FRANCE

A. Summary of activity and news

2012 saw an increase in activity and many initiatives by the CNIL (the French data protection authority) to support stakeholders, both public and private, in their conformity approaches.

The draft European Regulation: a major challenge for France

On 25 January 2012, the European Commission proposed a two-part reform of the 1995 Data Protection Directive: a proposal for a Regulation defining a general framework and a proposal for a Directive relating to data processed for police and legal purposes.

Although the CNIL subscribes to the objectives of this reform (reinforced personal consent, recognition of a data "portability" right, simplified administrative procedures for companies), it does have questions as regards the effectiveness of the system, and in particular protection of personal data.

It has therefore put forward a new governance model. Indeed, the aim is to guarantee citizens local control and to take into account the need for a one-stop shop for companies deploying cross-border processing.

To this end, the authorities must remain competent to perform all of their missions based on two criteria: the establishment of the data controller/subcontractor or the target audience.

The appointment of a lead authority based on the main establishment criterion ensures that there is cooperation between the competent authorities. This lead authority does not have exclusive competence, but rather its job is to instruct and coordinate. Decisions are adopted within the context of a joint decision-making procedure, with the agreement of the other authorities involved, whose independence is also preserved. The EDPS (European Data Protection Supervisor) is only involved in the event of disagreement between the authorities or to guarantee uniform interpretation of the Regulation.

The effectiveness of the proposed system lies in the restrictive nature of the final decision and in the guarantee of an effective right to appeal. Indeed, as decisions are approved by the competent authorities, the people involved can appeal to their national administrative jurisdiction against decisions made by their authority that are not in their interests. Similarly, companies may appeal to the jurisdictions in the country of the lead authority.

It is also seen as essential to maintain control over transfers, based on clearly defined rules, and to eliminate the possibility of using instruments of no legal value to manage these transfers.

The CNIL has also continued its exchanges with the European Commission in order to demonstrate its concerns and raise awareness within the Foreign Affairs Commission of the National Assembly and the European Affairs Commission of the Senate. As a result the two assemblies expressed, in a European Resolution, reservations about the proposed Regulation with regard to competence rules, adopting the same position as the CNIL. Discussions with the French government also continued throughout 2012.

Digital education/The main actions undertaken by the CNIL

In 2012, the CNIL decided to make digital education a strategic priority, reinforcing its action with the creation of new tools and wider distribution. Within this context, it performed several actions in 2012:

- Enhancement of the dedicated site (jeunes.cnil.fr) on which educational sheets are available
- Creation of a serious game on social media
- Issue of "Data Protection training" certificates

- Trainer training, for both consumer associations and chambers of commerce and industry, as relay points for companies.

Monitoring of technological developments

The cloud

Following a public consultation in 2011, the CNIL published a collection of recommendations in June 2012 for bodies wanting to use cloud services, in particular SMEs.

These recommendations are combined with contract clause templates that can be inserted into cloud computing service contracts to cover questions associated with personal data protection.

Smart meters

The CNIL has spent over two years discussing these meters, in particular studying their impact on privacy. In light of these privacy risks, in 2012, the Commission adopted a first recommendation to manage the use of smart meters.

This recommendation is based on the principle that the load curve cannot be collected systematically, but only when this is justified for carrying out work on the network or if the subscriber expressly requests it to benefit from specific services.

It also lays down a certain number of safety requirements, serious guarantees that must be given to ensure the confidentiality of data (e.g. performance of privacy impact studies before meters are deployed and risk analyses to determine the appropriate technical measures to put in place).

Google

Following Google's announcement in January 2012 regarding the entry into force of new confidentiality rules and new usage conditions applicable to almost all of its services, the CNIL, appointed by the G29, has examined these new rules.

Within the context of this mission, it sent two questionnaires to Google. Based on an analysis of the responses given and following examination of various documents and technical mechanisms, the G29 produced its recommendations in the form of a letter sent to Google on 16 October 2012 and signed by the 27 European data protection authorities.

Inspection actions

Notification of personal data breaches

When the "Telecommunications Packet" Directives were revised in 2009, the European legislator imposed on electronic communications service providers the obligation to notify personal data breaches to the competent national authorities and, in certain cases, to the individuals concerned. This requirement was transposed into French law by the Order of 24 August 2011 and its implementing decree of 30 March 2012.

A new mission was therefore entrusted to the CNIL, that of assessing the security level of systems belonging to electronic communications service providers and helping them to implement effective protection against data breaches. Lastly, depending on the severity of a breach, it can demand that providers notify the individuals concerned.

From March to December 2012, the CNIL received around 15 notifications.

Single record of prior convictions (TAJ)

The CNIL issued an opinion on the draft Decree creating a single record of prior convictions. The purpose of this file, shared by the police force and the national Gendarmerie, is to make it easier to check for offences, gather evidence and pursue those responsible.

Although it provides new guarantees for individuals, some reservations have been raised by the CNIL, which feels that major work is required to update the data in the original files before they are merged.

Furthermore, at the end of 2012, the CNIL carried out a thorough inspection (20 on-site checks and 60 inspections of items) of records of prior convictions.

Organisation	French Data Protection Authority
Chair and/or College	**Chair**: Isabelle FALQUE-PIERROTIN, **Vice-Chairmen**: 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 2012 (in million EUR): 17.2**
Staff	**Number of staff**: **171**
General Activity	
Decisions, opinions, recommendations	**2 078 decisions** (+ 5.5 % more than in 2011) **/ 113 opinions / 2 recommendations**
Notifications	**88 990** notifications to the CNIL, including: **8 946** notifications for video-surveillance systems (+49.3 % more than in 2011) **5 483** notifications for geolocation systems (+ 22.3 % more than in 2010)
Prior checks	**Authorisations: 1 534** in 2012, including: **316** authorisations adopted in the Plenary, **950** data transfer authorisations to non-EU States, **3** framework authorisations, **795** authorisations for biometric systems (+ 6.8 % more than in 2011), **658** authorisations for processing personal data for the purpose of medical research, and **162** authorisations for processing 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 2012, the CNIL received **35 924** writings and **134 231** calls
Complaints from data subjects	The CNIL received **6 017** complaints in 2012 (+ 4.9 % more than in 2011). This is the higher number of complaints ever received by the CNIL. The main issues of complaints are related to the right to be

	forgotten and to video-surveillance systems. **Requests from data subjects: 3 682** requests for indirect access where processing involves State security, defence or public safety (+ 75 % more than in 2011).
Advice requested by parliament or government	**In 2012,** the CNIL adopted **113 opinions**. Furthermore, the CNIL had meetings and was **auditioned 22** times by the Members of the French Parliament for an exchange of views about data protection issues.
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	**458** investigations (+19 % more than in 2011), including **173** investigations related to video-surveillance systems.
Sanction Activities	
Sanctions	**13 Sanctions taken by the CNIL in 2012.** **Legal actions against data controllers 56: (43** formal notices to comply, **4** financial penalties, **9** warnings), **2** discharges.
Penalties	**Total amount EUR 16 001**, imposed by the CNIL in **2012**
DPOs	
Figures on DPOs	**10 709** bodies appointed a DPO (+24 % more than in 2011).

B. Information on case-law

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

- Supreme Court of Appeal, social chamber, M. G. v Société Groupe Progrès 10208450 (04/04/2012)
- Supreme Court of Appeal, civil chamber 2, M. X. v Nouvelle du Journal de l'Humanité (12/04/2012)
- Supreme Court of Appeal, civil chamber, Aufeminin.com v Google France 1115188 (12/07/2012)
- Supreme Court of Appeal, civil chamber, Google France v Bac films (12/06/2012)
- Supreme Court of Appeal, commercial, financial and economic chamber, eBay Inc, eBay International v LVMH and others (03/05/2012)
- Supreme Court of Appeal, criminal chamber Damien 1180801 (06/03/2012)
- Supreme Court of Appeal, social chamber, Boymond v Société Technique française du nettoyage 1023482 (10/01/2012)
- Supreme Court of Appeal, social chamber, M. G. v Société Groupe Progrès 1020845 (04/04/2012)
- Supreme Court of Appeal, social chamber, M. X. v Association Perce-neige (10/05/2012)

- Supreme Court of Appeal, social chamber, M. X. v Nouvelle communication téléphonique (10/05/2012)
- Supreme Court of Appeal, social chamber, M. X. v SAS Helpevia 1115310 (26/06/2012)
- Supreme Court of Appeal, social chamber, Mrs. X. v Société Réunion fixations 1023521 (23/05/2012)

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 the Data Protection Authority. On the level of federal states ('Länder') there are the offices of the Länder Data Protection Commissioners, and additionally in Bavaria a separate supervisory authority with regard to the private sector.

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

Organisation	Federal Commissioner for Data Protection and Freedom of Information
Chair and/or College	Peter Schaar, Federal Commissioner
Budget	EUR 9 125 000
Staff	86 Data Protection: 82; Freedom of Information: 4
General Activity	
Decisions, opinions, recommendations	n/a
Notifications	n/a
Prior checks	n/a
Requests from data subjects	8 173
Complaints from data subjects	4 568
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	vgl. TB 2012 - n/a
DPOs	
Figures on DPOs	n/a

B. Information on case-law

1) Federal Fiscal Court sees tax identification number as compatible with the fundamental right to informational self-determination

The Federal Fiscal Court (BFH) has ruled that the tax identification number, which was launched in 2008, is constitutional because the public interest in consistent taxation justifies infringement of the right to informational self-determination (BFH, judgment of 18 January 2012, II R 49/10), although the strict principle of purpose and necessity must be observed. The legislature is therefore not free to extend the use of the tax identification number as it desires, as there are strict limits arising from the data protection requirements, which are also laid down in Section 139b(2) to (5) of the Fiscal Code. The Federal Constitutional Court has not yet had an opportunity to decide on the constitutionality of the tax identification number, so a final decision is still pending.

2) The judgment by the Federal Constitutional Court regarding the anti-terror file (1 BvR1215/07 of 24.04.2013) is of fundamental importance. Among other things, it contains the following key statements:

I. The European Court of Justice is not the lawful judge within the meaning of Article 101(1) of the Basic Law for matters relating exclusively to German basic rights. The applicability of EU fundamental rights is excluded from the outset if a national law internally pursues specific objectives which can only indirectly affect the functioning of legal relationships ordered under Union law. In these cases, there is no need for a preliminary ruling under Article 267 TFEU to clarify the extent of protection of fundamental rights under Union law.

II. A principle of informational separation derives from the fundamental right to informational self-determination. Accordingly, data may not generally be shared between intelligence services and police authorities. Restrictions are only permitted in exceptional cases. The exchange of data between intelligence services and police authorities for possible operational deployment must generally serve an overriding public interest which justifies access to the information under the easier conditions allowed to the intelligence services.

III. The collection and processing of contact data is only permitted under very restrictive conditions – irrespective of whether the contact person is aware of the action by the principal assigned to them or not.

IV. The executive has to extensively document and disclose internal decision-making and classification criteria – for monitoring by the data protection officer – also.

V. Supervisory control, including by the data protection officers, is crucially important and provides statutory support to the subjective rights enforced by the courts. A legally and/or actually inadequate system of supervisory control may justify disproportionate interference with the right of the data subject to informational self-determination. Essential prerequisites for efficient supervision include supervisory authorities with effective powers, full logging of accesses and changes to the data, and the ability to retrieve the data in practice, which must be assured by technical and organisational measures.

VI. Data protection officers are authorised to cooperate and to support each other, e.g. by way of administrative assistance through delegation or authorisation in the exercise of their powers. Effective interaction between the various supervisory authorities must be maintained– in practice– also.

VII. Regular mandatory checks laid down by law, which must be performed every two years or so at the latest, are also necessary for efficient supervision.

VIII. The legislature is urged to check and, if necessary, amend existing data transmission regulations with a view to safeguarding these principles.

3) Decision by the Federal Constitutional Court on the storage and use of telecommunications data

In a decision of 24 January 2012, the Federal Constitutional Court ruled that, with any request for telecommunications data, there must always be an authorisation to transmit the data and a justification for requesting it (the 'double-door model'). For this reason, the storage and forwarding of telecommunications data to investigating authorities was prohibited as non-constitutional, because these authorities were previously permitted access to passwords and PIN numbers. As a result, the investigating authorities were previously able to access a seized mobile phone and to search saved data without it being certain that its use by the authorities was even permitted.

The Federal Constitutional Court also ruled that a request for information about the subscribers behind a dynamic IP address constituted a breach of telecommunications secrecy. In order to identify a dynamic IP address, the telecommunications companies have to inspect their customers' call data, which means accessing specific telecommunications that are subject to protection under Article 10 of the Basic Law. The German legislature must establish a clear provision here to guarantee protection of the extremely sensitive telecommunications traffic data.

C. Other important information

FATCA

The Foreign Account Tax Compliance Act (FATCA), which entered into force in March 2010, is an American law for collecting assets in bank accounts abroad (outside the USA) of persons and companies liable for tax in the USA. The core of the FATCA is formed by enhanced notification and reporting duties for banks and other financial institutions abroad (Foreign Financial Institutions — FFIs) to the American tax authority (Internal Revenue Service — IRS). Substantial withholding tax deductions may be imposed if the notification and reporting duties are not observed.

Dealing with FATCA raised significant data protection issues. For example, the question arose as to whether the transmissions to the IRS are subject to the statutory rules in Sections 4b and 4c of the Federal Data Protection Act (BDSG) or to consent alone. To resolve this, France, Italy, Spain, the United Kingdom and Germany have settled on a model agreement with the USA, which is designed to serve as the basis for bilateral agreements.

The model agreement was presented on 26 July 2012. In it, the five countries undertake to collect the information about bank accounts held for US customers from the financial institutions domiciled in their territories and to forward it to the US authorities. In return, the USA agrees to exempt all financial institutions of the respective treaty partners from the requirement to conclude agreements with the IRS. This model agreement creates a framework for the reporting of account data by the financial institutions to their respective national tax authorities and the subsequent exchange of the respective data as part of the existing bilateral double taxation treaties.

The FATCA agreement (Agreement to improve international tax compliance and in respect of the American disclosure and reporting provisions known as the Foreign Account Tax Compliance Act) between the USA and Germany was signed by representatives of the Federal Republic of Germany and the USA on 31 May 2013 and has been ratified by an Act of Parliament. It is primarily based on the aforementioned model agreement of 26 July 2012.

During the negotiations, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) campaigned for the core requirements of data protection legislation. In particular, this involved creating a permissive rule for the financial institutions under data protection law, specifying the intended use of the personal data transmitted and standardising procedural and organisational safeguards.

Contrary to the urging of the BfDI, however, the procedural safeguards and the technical and organisational data security measures are regulated in a simple implementation agreement to the treaty.

The FATCA agreement now envisages a restriction on use and an assurance of confidentiality for the data to be used. The BfDI also urged that a permissive rule for the financial institutions required to send the details should be created by the inclusion of a planned Section 117c German Fiscal Code (AO), providing for restrictions on data processing on the principle of limitation of use and necessity. Consequently, German financial institutions have an enabling provision for data transmission.

The duties of the financial institutions are to be defined in detail by a statutory instrument based on Section 117c German Fiscal Code.

GREECE

A. Summary of activities and news:

The Hellenic Parliament passed Law 4070/2012, which, amongst others transposes Directive 2009/136/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Additionally, as it had been stated in the 15th Annual Report of the Article 29 Working Party on Data Protection, 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 Hellenic Data Protection Authority (hereinafter HDPA).

Once again, however, the serious problem of understaffing which the HDPA has been going through since its establishment could not be addressed in the year 2012 due to the ongoing public financial situation. Moreover, the continuous decrease of the budget that is being granted to the HDPA for operational needs has restrained the Authority's ability to sufficiently meet its obligations.

The HDPA issued this year, in total, 194 decisions and 5 opinions (some of which are briefly presented in Section B, Information on case-law).

In addition, the HDPA expressed in writing its views on a) the creation of an integrated Citizens' Register, that is the interconnection of registers of the Ministry of Finance, of Labour and Social Security, Ministry of Public Order and Citizen's Protection and Ministry of Interior, b) the new framework for e-government services, c) the Draft Regulation on electronic signatures and other related trust services repealing Directive 1999/93/EC, and d) the new legal framework on the protection of personal data — has been invited in parliamentary hearing.

Moreover, on the occasion of the European Data Protection Day 2012, the HDPA added new sections to its website, revised the content thoroughly and improved the entire structure. Aiming at raising awareness, the Authority, also launched a newsletter which provides information about current developments in the field of personal data on national, European and international levels. Finally, in order to plan new outreach activities, the HDPA created and conducted an online survey — on its website — on issues related to the protection of personal data.

Organisation	Hellenic Data Protection Authority
Chair and/or College	Petros Christoforos (President of the College).
Budget	EUR 2 213 787
Staff	Auditors Department: 15 lawyers and 11 IT experts (of them: three (3) on unpaid leave and one (1) resigned), Communications and PR department: 5 (of them: two (2) seconded for part of the year to other bodies/agencies of the civil service, one (1) on maternity leave), Human Resources & Finance Department: 16 (of them one (1) transferred to another civil service body.
General Activity	

Decisions, opinions, recommendations	The HDPA issued in total 194 decisions and 5 opinions.
Notifications	The HDPA received 540 notifications (335 concerned installation and operation of CCTVs and 57 data transfers to countries outside the E.U.).
Prior checks	The HDPA issued or renewed 81 permits concerning the processing of sensitive data, interconnections of files and data transfers to third countries without an adequate level of protection.
Requests from data subjects	989
Complaints from data subjects	675 (Prosecution Authorities and Public Order: 8, National Defence: 1, Public Administration and Local Government: 24, Taxation-Ministry of Finance: 6, Health: 13, Social Security: 4, Education and Research: 4, Banking: 75, Private Economy: 64, E-communications: 254, Work Relations: 20, Mass Media: 23, Other: 179).
Advice requested by parliament or government	4 - see Section (a) 'summary of activities and news'
Other relevant general activity information	On European Data Protection Day 2012, the HDPA added new sections to its website ('law enforcement authorities-security', 'taxation', 'social security', 'new technologies', 'education-research', 'health' and 'finance'), revised the entire content and improved the structure. Aiming at raising awareness, the Authority launched a newsletter which provides information about current developments in the field of personal data on national, European and international levels. In order to plan new outreach activities, the HDPA created and conducted an online survey - on its website - on issues related to the protection of personal data.
Inspection Activities	
Inspections, investigations	11 inspections (of them 10: data controllers of private sector and more specifically companies that are in the business of buying/selling databases containing personal data, 1: in the National SIRENE Representation and the Schengen Information System (SIS)). Two (2) special inspections were conducted on the operation of CCTV systems in a company and in an NGO. Four (4) other inspections that had begun in 2011 were completed in 2012 (3: on the protection and security of personal data that are held and processed by specific electronic systems and services at the Ministry of Education — see the case-law, 1: on the online prescription system of the General Secretariat of Social Security, Ministry of Employment and Social Protection.
Sanction Activities	
Sanctions	38 sanctions (5 warnings, 33 fines) were imposed by the DPA in

	regarding the following thematic areas: Public Sector (1), Health care (5), European-International (1), Financial Sector (14), Personal Data Breaches (8), Mass Media (3), Education and Research (1) and Electronic Communications (4). In three decisions the HDPA imposed a warning and a fine.
Penalties	Fines: Amounts: EUR 2 500-50 000 (total EUR 486 500) were imposed by the HDPA.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Opinion 3/2012

An opinion was delivered by the HDPA concerning the requirements for entering and deleting aliens in the SIS on the basis of Article 96 of the Schengen Agreement and in the National Record of Unwanted Aliens. The Authority judged that entering an alien in the National Record does not entail an *ipso jure* alert in the SIS. Entering an alien in the SIS is carried out according to the requirements of Article 96 of the Schengen Agreement. The deportation by administrative or judicial authorities in accordance with national law justifies an alert in the National Record and the SIS. An alien is entered in the SIS if s/he has been convicted by a national court of an offence carrying a penalty involving the deprivation of liberty of at least one (1) year. Entering an alien in the SIS is justified if there are serious grounds that the person concerned committed or intends to commit serious criminal offences. Also, entering an alien in the National Record is justified because of administrative expulsion on specific grounds and if the presence of the alien is rightfully dangerous for the public order and security of the country. An alien is deleted from the SIS after a period of three years from the alert and if there is no justified decision for retaining it.

Decision 36/2012

The HDPA deemed that the publication in a newspaper of a photograph showing a mother with her under-aged daughter, without their prior consent, in the context of an article on endometriosis constitutes illegal processing, collection and preservation of personal data. The Authority concluded that the photograph is irrelevant to the content of the article and it might create the impression to the average reader that the mother suffers from the above-mentioned condition. It imposed a fine on the data controller, ordered the deletion of these data from the newspaper archives and banned their republication.

Decision 112/2012

The HDPA examined a number of notifications regarding geolocation (using GPS technology) and 24-hour surveillance services provided by two companies. The subscribers to those services are able to determine the features of the service and spot the geographical position of the geolocation device holder. These services involve, especially, people with health problems or whose duty is to look after people with such problems, as well as parents of minors, for personal safety reasons. The processing of the device holder's data includes geolocation, demographic and sensitive health data. The HDPA's Decision set out specific terms and conditions for the protection of personal data deriving from such geolocation services, such as: the data controller must provide adequate information to the device holder on the processing of, access to and security measures of the latter's data; in some cases the data must be encrypted and/or protected by security measures; also, the device holder must have been notified and have provided his/her consent in advance; additionally, for sensitive data the consent must be written; if the device holder is a person under

a legal incapacity, the consent is provided by the litigation guardian; in case of minors, consent must be given by the parents/guardians, yet minors' opinions must be taken into account; the device holder must be provided the ability to exercise the right to object; the use of this system on minors must first be evaluated, in terms of risk, by the competent state authorities and until then, it can only be used for health reasons.

Decision 117/2012

A political organisation published a poster showing in the background — without their consent — a group of people protesting in a demonstration. The HDPA judged that the picture of this group of people was not directly related to the content of the poster and might erroneously lead the average citizen to think that these people are followers of the said political organisation. As a result, the Authority imposed a sanction on the organisation, prohibited the republishing of the poster and ordered its deletion.

Decision 165/2012

The Authority judged that the publication of sensitive personal data (concerning criminal charges) in the electronic edition of a newspaper (on its website) is against the Law 2427/1997 on personal data protection. More particularly, the HDPA deemed that the illegal publication of sensitive personal data on the Internet — via a search engine — disproportionately violates the data subject's rights because, by means of such a processing, the data subject is always associated with a past behaviour and thus the relevant information becomes easily accessible to anyone that is searching for it — and not only to journalists, researchers and scholars. Moreover, the HDPA imposed a fine on the data controller, ordered that the data concerning the data subject published on the newspaper website be anonymised, so that even when searching by the publication date, it will not be possible to identify the data subject, and issued a warning (to the data controller) in order to examine the data subject's right to object and either anonymise the data or reject such claims providing specific reasons.

Decision 187/2012

The HDPA issued a warning to the Ministry of Education to comply with the recommendations that were specified in its Report after the completion of three inspections of the electronic systems 'electronic service of issuance of special ticket/student identity card', 'e-school' and 'e-data centre' regarding the protection and security of personal data that are held and processed by these systems. In particular, the Authority found out specific deficiencies and/or omissions by the data controller in the procedures and the organisation of security, the sufficient documentation of the security measures applied and their systematic monitoring, the authentication of users, the management and support of these systems and finally the general obligations according to the Law 2472/1997.

HUNGARY

A. Summary of activities and news:

Organisation	National Authority for Data Protection and Freedom of Information
Chair and/or College	Dr Attila Péterfalvi
Budget	HUF 390 211 000
Staff	59
General Activity	
Decisions, opinions, recommendations	2 152 (DP: 1 825, FOI: 327)
Notifications	12 166
Prior checks	Data protection audit investigations are allowed by law from 1 January 2013.
Requests from data subjects	1 388 (DP: 1 212; FOI: 176)
Complaints from data subjects	764
Advice requested by parliament or government	207 + 46 (incentives for legal amendments)
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	2 152
Sanction Activities	
Sanctions	
Penalties	11
DPOs	
Figures on DPOs	Organisation of Conference of DPOs (June 2012)

B. Information on case-law

B1) unlawful data processing - provider of website (www.ingatlandepo.com and www.ingatlanbazar.com)

The Hungarian DPA imposed a fine — of HUF 10 000 000; currently the highest amount possible by law — on a website provider company (hereinafter referred to as the Defendant). Contracts were concluded between Hungarian data subjects (hereinafter referred to as the Claimants) and the Defendant with the purpose of advertising real estates on behalf of the Claimants on the website of the Defendant.

Once the real estates were sold, the advertisements expired or the Claimants simply wished to delete, or have the Defendant delete, their ads, they failed to do so. Despite their strong and repeated requests the Defendant failed to delete the advertisements at all. Moreover the Defendant passed on the personal data of the Claimants to — among others — claim management companies.

Numerous complaints were received by the Hungarian DPA with respect to the above issues. As a result the DPA launched an investigation procedure and called up the Defendant to make statements on its behaviour within a certain period of time. Since the Defendant missed the deadline set by the DPA and proved to be unwilling to cooperate in the procedure the DPA launched a data protection procedure.

As a result of the data protection procedure the DPA concluded that the Defendant had violated the privacy rights of the Claimants on multiple counts. Among others the Defendant infringed the principle of proportionality, the right for information, the right of 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 ignored the multiple objections made by the Claimants in line with the data processing of the Defendant. Therefore the Defendant lacked the essential legal basis for various data processing activities.

As a consequence, the Authority - with regard to the size of the scope of individuals affected by the legal offence, its weight and repetition along with the reluctance of Defendant to cooperate with the competent state authorities and stakeholders concerned - decided to impose a fine as well as disclosed its decision to protect the rights of a greater number of data subjects.

The case is still pending.

B2) Google Street View (GSV)

Following numerous consultations with the representatives of Google Inc. (service provider of GSV) and several investigations carried out by the former Data Protection Commissioner dated back to 2009 as well as taking into consideration the recent rulings (C-468/10. and C-469/10.) of the ECJ the NAIH issued a statement in which it approved the launch of GSV service in Hungary provided that Google complies with the relevant data protection principles and preconditions (including, among others, prior notification to the public; enabling for data subjects to submit requests for deletion; blurring of personal data as soon as possible etc.) set forth by NAIH in its statement.

B3) Application of CCTV devices in workplaces

Numerous petitions were received by both the NAIH and the former Data Protection Commissioner (hereinafter referred to as DP Commissioner) in recent years in which the applicants complained about the widespread application of CCTV surveillance devices in workplaces.

From 2012 both the former Labour Code and the DP Act of 1992 have been repealed by new legal instruments. The new Labour Code, effective as of 1 July 2012, already includes governing provisions (§§ 9 and 11) that are to be taken into consideration for CCTV devices in workplaces. These general provisions can lead, however, to different enforcement of the right of informational self-determination.

As a result of a thorough investigation we issued a recommendation in which we proposed guidelines to the employers with the objective of enabling them to comply with data protection legal requirements on workplaces.

B4) Biometric identification

A client in her submission requested the Authority to deliver an official statement as to whether the data processing of a school could be lawful where the education institution intends to install a biometric identification system at entry points.

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

Fingerprints of a natural person qualify as personal data and taking of fingerprints qualify as data processing. Both the relevant national legislation and the EU Data Protection Directive stipulates fundamental legal principles which should also be regarded in data processing activities. These include e.g. the principle of proportionality (et al.).

The Authority found that a biometrics system — aimed at taking fingerprints of pupils upon entering the school — for the purpose of personal security and the protection of property does not meet the requirements of proportionality. Better identification, instead, could be secured by any other — more harmless and less intrusive to privacy — ways.

Consequently the introduction of such an entry system would jeopardise the privacy rights of the data subjects concerned.

B5) Cloud computing

A political association lodged a petition with the Authority and requested its statement on the lawfulness of the association's data processing activity. The association (hereafter: data controller) indicated its wish to process the personal data of their supporters by means of cloud computing technology. They added that they plan to choose a cloud computing service provider of which the parent company is registered in the US whilst it has a subsidiary in Ireland. The service provider in question is said to be on the safe harbour list published by the U.S. Department of Commerce.

The Authority found that the sensitive nature of the personal data of supporters of a politically active association significantly increases the security concerns. Therefore the Authority opposed the transfer of such personal data to the 'cloud'.

B6) Hacking of Website of Capital Mineral Water and Beverage Co. Ltd.

In October 2012 a Turkish hacker group was said to have compromised the Internet promotion site of the above company. As a result more than 50 000 personal data items (name, e-mail address, date of birth etc.) were stolen. On this occasion our Authority delivered an announcement in which we questioned why the personal data of consumers had been made accessible online or why these personal data had not been encrypted. Simultaneously we called for higher consideration of data security measures to be introduced and applied in order to avoid similar data breaches.

In this matter a data protection administrative procedure is still in progress.

B7) Financial penalty to an Internet publishing company

We have received a complaint from an individual stating that s/he has been getting unsolicited marketing e-mails from a company to which s/he has not consented as well as the company failed to terminate the service and to delete the contact details of the complainant despite his/her continuous requests to do so.

As a result of an investigation and afterwards a data protection administrative procedure the Authority imposed a financial penalty of HUF 3 million. This huge amount had been decided due to the following aggravating requirements: the wide scope of persons affected by the unlawful processing; the high number of minors concerned; the severity of the infringement as well as the extraordinary duration of the unlawful situation. Extenuating circumstances had also been taken into consideration as follows: the finalisation of a new privacy policy; making it accessible on the website and the reporting of amendments into the data protection registry. This willingness of the controller to cooperate with the Authority was demonstrated by the velocity with which the controller performed the necessary modifications that were made right after the data protection procedure had been initiated.

B8) Data processing of dating websites

The NAIH investigated a case in which a Hungarian company (company), an operator of approximately 40 websites, was imposed to pay a data protection fine of HUF 3 million mainly because of violation of the rights of minors and because of the unlawful data processing activities related — among others — to e-mail marketing services offered. The case was opened upon a complaint by a citizen against the company in which he claimed that he was continuously receiving e-mails containing advertisements without his consent, that the company did not delete his data after they were requested to do so and even then continued to send the company newsletters.

In its proceedings the NAIH found out that on the websites, operated by the company, the details of data processing, including transfer of data given during the registration to third parties were not clear. There was no possibility guaranteed to the users for giving their free and deliberate consent for receiving marketing e-mails as the consent was considered automatic with the registration. Furthermore, the NAIH showed that information on the purpose of data processing was inadequate and there was no possibility for the users to sign off from newsletters sent by the company. During the investigation on the matter the NAIH also found an additional, rather worrisome issue, namely the mismanaged registration of minors especially on dating websites.

The legal bases on which the NAIH founded its decision were Act CXII of 2011 on Informational Self-determination and Freedom of Information, Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers, Act CVIII of 2001 on electronic commerce and Act IV of 1959 on the Civil Code. The NAIH also took into consideration the findings of Opinions 5/2004, 5/2009, 15/2011 of the Article 29 Working Party on online social networking, Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and online information services industry and the Report COM(2011) 556 of the European Commission on protecting children in a digital world.

The NAIH - among other smaller-scale issues - concluded its administrative procedure by stating that the data processing activities of the company were not in harmony with the above-mentioned legislative and non-legislative acts. It seriously endangered the minors' rights to protection as it completely omitted requesting the necessary consent from the legal representatives (parents) of the minors. It has moreover violated the data subjects' rights to data protection by not ensuring the possibility of an adequate procedure during the registration where a free and deliberate consent should be asked and given for the transfer of the data subjects' e-mail ID for marketing purposes and for receiving marketing e-mails. It has furthermore not provided clear information on data protection rules and procedures and it did not provide a possibility for signing off from receiving the newsletter of the company. As for the e-mail marketing practices of the companies, the NAIH in its deliberation suggested using the so called opt-in solution, when a separate and dedicated check box is used during the registration.

B9) Data processing of a discount purchasing system

The NAIH received a complaint of a natural person in relation to the allegedly wrongful data processing activity of a marketing agent company (hereinafter referred to as the company). The company was operating a discount card system by means of which the registered members were entitled to purchase ítems at lower prices from certain entrepreneurs. Registering into the system was possible exclusively upon an invitation by a member who had registered previously. The active members, upon obtaining new members, were receiving allowances for recruiting freshmen. Later the Authority received complaints from members stating that the system was not functioning in compliance with the effective data protection rules. At first the Authority launched an investigation procedure with a view to get an insight into the facts. As the data controller failed to reply to several approaches the NAIH decided to initiate a data protection administrative procedure. In its procedures the NAIH concluded that the data controller had failed to compose a comprehensive and easy-to-understand privacy policy thus disabling the clients from becoming aware of their rights and to render a freely given consent to the data processing of their own personal data by the data controller.

C. Other important information

Major legislative changes

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 was tasked with the responsibilities mentioned previously, it commenced 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 Parliament the 11 July 2011 and took effect on 1 January 2012.

Some provisions of the new Hungarian Privacy Act (Act CXII of 2011 on Informational Self-determination and Freedom of Information; in effect as of 1 January 2012) governing the mandate of the President of the Hungarian DPA (hereinafter referred to as the President) - considering also the critical remarks from the European Commission - were significantly modified in order to strengthen the independence of the position of the President (amending act: Act XXV of 2012). Below are specified the amendments that had been made accordingly.

- In those cases where the conclusion on the termination of mandate of the President shall be ascertained by the President of Hungary at the written motion of the Prime Minister the President shall have the right to challenge this motion before court. The action shall be lodged against the Prime Minister. Reason for this modification was that the mandate of the President shall terminate only if the motion from the Prime Minister is undoubtedly lawful and factually well-grounded.
- The modification entitles the President to participate and address the session of the Parliamentary Committees hence empowering him to inform the deputies on his activity, as well as to make suggestions concerning the legislative process and bills.
- Another amendment stipulated that the President shall have - beyond further additional conditions - at least ten years of professional experience in supervising proceedings related to data protection or freedom of information. Pursuant to the former regulations five years of professional experience had been sufficient.

IRELAND

A. Summary of activities and news:

In 2012, the Office of the Data Protection Commissioner opened 1 349 formal complaints for investigation (many complaints are dealt with informally by providing the complainant with appropriate information on their rights). 864 investigations of complaints were concluded in 2012. As in previous years, the vast majority of complaints were resolved amicably, with only 36 complaints giving rise to formal decisions. The first prosecutions were taken against telecommunications companies for failure to comply with the new security and breach notification requirements under Statutory Instrument 336 of 2011 (which transposes Directives 2002/58/EC, as amended by Directives 2006/24/EC and 2009/136/EC in Ireland). Information in regard to prosecutions in 2012 is included in Section B of this report. Personal data security breach notifications to the Office continued to increase (1592 in 2012), in line with the trend since the introduction of the Personal Data Security Breach Code of Practice in 2010.

Organisation	Office of the Data Protection Commissioner
Chair and/or College	Billy Hawkes
Budget	EUR 1 458 000 budget. EUR 1 552 468 expended.
Staff	28 at 31 December 2012.
General Activity	
Decisions, opinions, recommendations	36 formal decisions.
Notifications	5 338
Prior checks	N/A
Requests from data subjects	9 500 e-mail queries. Also queries in writing.
Complaints from data subjects	1 349
Advice requested by parliament or government	Regular informal consultation on legislative/regulatory proposals.
Other relevant general activity information	1 592 data security breach notifications.
Inspection Activities	
Inspections, investigations	40 audits (inspections)
Sanction Activities	
Sanctions	195 prosecutions against 11 entities.

Penalties	EUR 7 500 fines imposed plus costs. EUR 99 500 charitable donations ordered by the Court through application of the Probation Act, plus costs.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In most cases, in accordance with Section 10 of the Irish Data Protection Acts 1988 and 2003, complaints submitted to the Commissioner are resolved amicably without resort to a formal decision or enforcement action. Such amicable resolutions may, for example, involve a financial contribution by the relevant data controller to the data subject concerned or to an appropriate charity. Where necessary, enforcement powers are used — for example, when data controllers fail to respect the access rights of data subjects. In some cases, data controllers are named in case studies included in the Commissioner's Annual Report. In the course of 2012, 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 336 of 2011 (transposing Directives 2002/58/EC, as amended by 2006/24/EC and 2009/136/EC in Ireland). 195 prosecutions against 11 entities were taken in 2012. These included the first prosecutions taken against telecommunications companies for failure to comply with the new security and breach notification requirements under Statutory Instrument SI 336 of 2011, several prosecutions in relation to unsolicited marketing text messages and e-mails, and offences in relation to registration under the Data Protection Acts.

The High Court also ruled on appeal in relation to a point of law regarding access to data in a case where legal proceedings were in existence between the parties. The High Court ruled that: 'the existence of proceedings between a data requester and the data controller does not preclude the data requester making an access request under the Act nor justifies the data controller in refusing the request.' In another appeal to the High Court, the High Court upheld the Commissioner's decision not to investigate a complaint which he found to be 'frivolous or vexatious' and confirmed that the higher courts had no jurisdiction for an appeal, as no investigation had taken place.

C. Other important information

The Commissioner continued to engage with large public sector organisations about the extent of data sharing in the public sector. A report on the Office's investigation into INFOSYS, a data sharing system in the Irish public sector was published as an annex to the 2012 Annual Report of the Office. The investigation revealed a failure of governance in some of the public sector organisations audited, and recommendations for improved governance were made, including in relation to greater transparency and improved access and security controls.

In recognition of the increased responsibilities which are likely to fall to the Office, when the legislative proposals on data protection currently under discussion in the Council of Ministers of the European Union and European Parliament are passed into law, extra staffing was allocated to the Office at the end of 2012. These resources included a Chief Technology Advisor and a Legal Advisor, as well as additional administrative staff. The non-pay budget allocation to the Office for 2013 was also increased.

ITALY

A. Summary of activities and news:

The new collegiate panel of the Italian DPA took office on the 19 June 2012, replacing the panel headed by Prof. Francesco Pizzetti (2005-12). The new Commission includes Mr Antonello Soro, President, Ms. Augusta Iannini, Vice-President, Ms. Giovanna Bianchi Clerici and Prof. Licia Califano, Members. Mr Giuseppe Busia is the new secretary general to the DPA.

Legislative Changes

Electronic Communications - Data Breach Notification

Directive 2009/136/EC was transposed into Italian law in the course of 2012. In particular, legislative decree No 69/2012 introduced the 'personal data breach' concept into our law and set forth the obligations to be fulfilled by providers of publicly available electronic communications services in case of such a breach (see Section 32 a of the Italian Data Protection Code — DP Code).

Additional legislative changes in this context concern the amendments made to a few definitions contained in the DP Code (the wording 'contracting party' was substituted for 'subscriber'); the rules on storage of and access to information in the contracting party's terminal equipment with particular regard to 'cookies' (Section 122 of the DP Code); the security measures and procedures to be implemented by providers of publicly available electronic communications services (set forth in Sections 32 and 132 a of the DP Code) and the corresponding amendments made to the applicable sanctions (under Section 162 b relating to 'personal data breaches').

'Simplification' Measures

Changes to DP legislation were also brought about by 'simplification' measures adopted urgently by the Italian Government (via a decree issued on 9 February 2012, which was then enacted with additional amendments via Law No 35 of 4 April 2012). As regards, in particular, security measures, the decree did away with the requirement for data controllers to draft a 'security policy document', which was replaced by a self-certified statement. Still under the decree in question, the Italian DPA was deprived of its power to lay down simplified arrangements for implementing minimal security measures via own measures.

The same decree allows processing judicial data in pursuance of memorandums of understanding as entered into by organisations with the Ministry for Home Affairs (or peripheral offices thereof) for preventing and countering organised crime - providing the categories of processed data and the processing operations to be performed are spelled out (see Sections 21(1 a) and 27 of the DP Code).

'Whistleblowing'

Under the newly introduced Section 54 a of legislative decree No 165/2001 ('Protection of Public Employees Reporting Illicit Conduct'), a public employee who becomes aware of illicit conduct in performing the respective tasks and reports such illicit conduct to judicial authorities, the Court of Auditors and/or his or her superordinate may not be punished, dismissed or subjected to discriminatory measures impacting his or her occupational conditions on whatever grounds related to the said reporting.

Key issues

The key issues addressed by the DPA in 2012 included topics that have come repeatedly to its attention over the years. Safeguards for data subjects in connection with telemarketing, privacy-friendly deployment of (smart) video surveillance equipment, occupational issues including the use of biometrics for access controls (found to be mostly excessive and disproportionate compared to the specific purposes) were among the leading cases addressed in 2012. Below is a summary of other issues entailing elements of novelty.

Personal Data Breaches

The Italian DPA laid down specific guidelines to clarify the notification obligations applying to telecom and Internet service providers in case of personal data breaches. The guidelines clarify who is required to notify a breach under what circumstances, whether and how to notify users and contracting parties, and what technical and organisational security measures have to be implemented (see Decision of 26 July 2012 as published in Italy's Official Journal No 183 of 7 August 2012 - Web Doc. No 1915485).

Forums, Blogs, Online Archives of Daily Newspapers

Guidelines for the fair processing of personal data by health-focused blogs, forums, social networks and websites were published in February 2012. The Guidelines do not apply to online health care or telemedicine services. The main recommendations are that website owners should inform users of the risks arising potentially from the posting and dissemination online of their health-related information; to that end, an ad-hoc 'risk notice' should be displayed on the home page.

Further to a decision by Italy's Court of Cassation (No 5525/2012) on the so-called 'right to be forgotten', the Italian DPA granted a complaint to have a news item updated as posted on the website of a leading daily - to take account of supervening developments. It should be noted that the specific news item had already been de-indexed. In particular, the publisher was ordered to flag - e.g. by posting a notice aside the individual news items - that there had been subsequent developments. By so doing, he would ensure that the data subject's personal identity would be respected whilst enabling readers to be informed reliably and accurately.

Authorisations: Genetic Data, Medical, Biomedical or Epidemiological Research

The general authorisation granted by the DPA to process genetic data was issued anew in December 2012 to take account of an opinion rendered to the Italian Ministry of Health along with the experience gathered and the contributions coming from authoritative experts; it was also granted to public and private mediation organisations in pursuance of the applicable legislation.

The general authorisation that had been issued provisionally in March 2012 to allow processing personal data for medical, biomedical and epidemiological research purposes without informing data subjects, under specific circumstances, was redrafted and expanded in December 2012. The authorisation now provides that medical data may be processed along with sex life, racial or ethnic origin information without the patients' consent if it is demonstrably impossible to inform patients of the processing either on 'ethical grounds' or because of 'organisational impediments'; additional conditions to be fulfilled in such cases include the favourable reasoned opinion rendered on the given research project by the competent ethics committee. For the remainder, patients' consent remains necessary and must be obtained immediately when they contact the given medical institution — in particular if they visit the outpatient clinic subsequently.

The International Dimension

The Italian DPA continued its active participation in the Article 29 Working Party. The DPA could also follow the debate in progress on the reformation of the EU data protection framework by participating through its experts in the Italian delegation at the DAPIX Working Party of the EU Council.

The DPA contributed to the work at both the OECD and the Council of Europe, in particular via the Working Party on Information Security and Privacy (WPISP) and the T-PD Advisory Committee and Bureau, respectively; the latter has been working for some time on the revision of Convention 108/1981. The DPA is a member of the joint supervisory authorities at EU level (Europol JSB, Schengen JSA, CIS, Eurodac co-ordination group) and also contributes regularly to and participates in the so-called Berlin Group (International Working Group on Data Protection in Telecommunications).

The DPA continued its work as part of the European Commission's IPA, TAIEX and Twinning programmes for newly accessed EU countries, candidate countries (Turkey, Croatia, FYROM), Balkan countries, Russia

and European Neighbourhood Policy countries, in order to facilitate approximation of the legislation in those countries to the EU's data protection framework.

Organisation	Italian Data Protection Authority
Chair and/or College	Chair of the College: Dr Antonello SORO College: Augusta IANNINI Giovanna BIANCHI CLERICI Licia CALIFANO
Budget	Approx. EUR 8.8 million (Funding by Government)
Staff	122
General Activity	
Decisions, opinions, recommendations	Number of decisions taken by the College: 440
Notifications	1 053
Prior checks	13
Requests from data subjects	Total number of requests: approx. 4 900 Requests for information ('quesiti'): 320 Reports and claims ('segnalazioni' and 'reclami' received in 2012) from data subjects: 4 592
Complaints from data subjects	(formal complaints, specifically regulated by the DP Code, concerning access to one's personal data): 233
Advice requested by parliament or government	opinions in reply to parliamentary inquiries: 6 opinions to Ministries and to the PM Office: 23 Topics: police, public security: 3 judicial activity: 2 e-government and databases: 6 education and training: 1 health care: 1 businesses: 1 exercise of rights: 2 welfare: 3 electronic documents: 2

Other relevant general activity information	The front office of the DPA received, in 2012, about 34 000 telephone calls and e-mails National authorisations for international transfers: 3
Inspection Activities	
Inspections, investigations	Number of inspections and/or investigations (on the spot): 395 (in 56 of which infringements having a criminal nature were reported to the judicial authority)
Sanction Activities	
Sanctions	Approx. 600
Penalties	Amount: approx. EUR 3.8 million imposed by financial police in charge of controls on the DPA's behalf
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Court of Cassation — Right to be forgotten and updating of news

A decision by the Court of Cassation (No 5525/2012) concerning a news item that was available online in the archive of a well-known daily found that the publisher was required to make sure that the given information was both placed against the relevant background and updated; this was intended to protect the data subject whilst providing the public with thorough, accurate information. Accordingly, the Court ordered the publisher to make arrangements so that the developments of the specific case — i.e. the fact that a final judicial decision had been rendered on the case — could be flagged alongside the original item, and to make such additional information easily and quickly available to users.

Court of Milan - Geographical Scope of Application of the DP Code

Ruling on the appeal lodged against a decision by the DPA of 7 April 2011, the Court of Milan addressed the concept of 'equipment' as set forth in Section 5(2) of the DP Code. In particular, the Court found that the concept of 'mere conveyance of communications' did not apply to the service provided by a marketing company that handled its ad messaging activities via servers located in the USA but then routed part of the faxes bound for Italy to a delivery node located in Italy; such delivery node was managed by a telephone company established in Italy. The delivery node in question was a complex IT facility, which forwarded to the sender a message on the (un)successful delivery of the individual faxes; such messages included the sender's IP address and fax number, the recipient's fax number, the outcome, the number of faxes sent and the contents of the given message(s). Thus, the system in question linked the Internet with the telephone network on the Italian territory via a specific device known as 'fax gateway', which operated by processing personal data. Given the above, the Court of Milan upheld the DPA's decision and ruled that the processing operations in question fell under the scope of application of the Italian DP Code.

Court of Cassation – Posting of public notices by a municipality

The Court of Cassation (by its Decision No 12726/2012) upheld a decision by the DPA of 9 December 2003 that addressed the inclusion of an employee's name on the public notice convening a meeting of a municipal board. The public posting of the notice - which related to an enforcement proceeding instituted against the employee - was found to be in line with the applicable legislation on local authorities (Legislative Decree No 267/2000), however the amount of personal information disclosed was ruled to be excessive and disproportionate compared to the transparency and information purposes sought by the municipality.

C. Other important information

Expressions of interest for the Italian State to appear in proceedings before the EU Court of Justice

The DPA expressed its interest for the Italian State to enter an appearance before the EU Court of Justice in the following cases:

– Case C-119/12 (request for a preliminary ruling under Article 267 TFEU) on interpretation of Article 6 of Directive 2002/58/EC, to support an interpretation of the said Article that should be in line with the way it was transposed into Italian law (see Section 123 of the DP Code). The provision in question specifies under what conditions traffic-related personal data may be processed for commercial (here: billing) purposes in accordance with data minimisation and proportionality principles and by striking the appropriate balance between the interests at issue.

– Case C-131/12 (request for a preliminary ruling under Article 267 TFEU) on interpretation of Articles 2, 4, 12 and 14 of Directive 95/46/EC with particular regard to the notions of establishment in a Member State's territory and 'use of equipment situated on the territory of the said Member State', as well as on storage of the information that is indexed by a search engines and the right to data erasure. It was submitted that cases similar to the one in whose respect the Spanish Audiencia Nacional applied to the EU Court of Justice had been addressed by the DPA by requesting the source websites (i.e. the controllers for the data that had been posted and then collected by search engines) to implement measures aimed at preventing external search engines from retrieving the data subjects' personal data. Such measures entail, in particular, compilation of the robots.txt file as per the 'Robots Exclusion Protocol' along with the use of 'Robots Meta Tags'.

LATVIA

A. Summary of activities and news:

Within the year 2012 the draft of amendments to the Personal Data Protection Law has been elaborated. Mainly the amendments relate to the following issues:

- Clarification of the definition of the controller, including the definition of joint-controller, by determining the rights and duties, as well as the shared responsibility;
- Determination of several more exemptions from notification;
- Specified requirements regarding data transfers to the third countries that do not ensure such data protection levels as found in Latvia;
- Requirement for the state and local government institutions to implement evaluation of the effectiveness of personal data protection;
- Determination of the rights of the Data State Inspectorate to determine a certain time frame when the information should be submitted to Data State Inspectorate in order to carry out its functions.

There have been also amendments elaborated regarding the Schengen Information System. The Data State Inspectorate of Latvia in cooperation with the Ministry of Justice has issued an opinion that it should be revaluated and reconsidered if all the institutions need access to SIS, and for which purposes.

At the national level the Data State Inspectorate of Latvia provided its opinion regarding the different legal acts and policy initiatives, listing the main ones below:

1) Draft Law on Credit Bureau;
2) Draft Law on Debt Retrieval;
3) Draft Law on the Electronic Identification.

In October 2012 Latvia had the Schengen evaluation regarding data protection and thus it was the priority of the office (several control activities were carried out, as well as information materials elaborated).

Considering the complaints received in 2011 and 2012, the Data State Inspectorate of Latvia has identified the following issues where the majority of complaints were received:

1) Personal data processing within the debt collection process;
2) The controller has not provided the necessary information to the data subject;
3) Publishing of personal data on the Internet.

There were 10 seminars organised, as well as three exams for the data protection officers. 12 persons have obtained the status of data protection officers.

Key topics where advice was requested from public authority

The Data State Inspectorate does not have any statistics available on the requests for advice submitted by public authorities. However it daily receives calls from different public authorities on a variety of issues related to personal data processing — starting with the necessity to notify the personal data processing, the data subject's access rights and following more complicated questions which require in-depth analysis in order to find out the best solution regarding personal data protection (for instance, there have been many questions raised by the public and private sector regarding the data processing aspects within the labour relations and data security issues, therefore the Data State Inspectorate of Latvia will elaborate recommendations on these issues in 2013).

Information on awareness-raising activity

The Data State Inspectorate has organised several seminars on issues for personal data protection, for different target audiences — for instance, educational establishments, local government institutions, bank and finance sector representatives, medical staff, etc. The Data State Inspectorate provides seminars which are open for all the persons interested.

There are at least four media requests each week regarding different data protection issues. Attention has been also paid by the media to the issues considered at the Article 29 Working Party, as well as to the outcome of the joint Baltic countries' investigations regarding personal data processing.

Since there were several control activities carried out regarding loyalty cards, there was media support on this issue by motivating people to think about their personal data as a value and to evaluate more careful which are the cases when personal data should not be submitted to the persons/companies that request it.

Organisation	Data State Inspectorate of Latvia (Datu valsts inspekcija)
Chair and/or College	Director — Signe Plūmiņa
Budget 2012	LVL 266 907 (approx. EUR 370 457)
Staff	19 (including the administrative and maintenance staff)
General Activity	
Decisions, opinions, recommendations	Regarding the statistics on decisions, opinions — N/A. Regarding recommendations — no recommendation elaborated in 2012; two recommendations foreseen in 2013
Notifications	352 (including the notifications on amendments to personal data processing)
Prior checks	234; focused on the risk areas (determined for each year) such as processing of sensitive data, biometric data processing (including video surveillance) and personal data transfer to third countries.
Requests from data subjects	N/A
Complaints from data subjects	Total number of investigations — 496 (80 % of investigations were carried out due to complaints received). 4 complaints from data subjects from third countries regarding their personal data processing within SIS. 11 complaints regarding SPAM (11 investigations carried out thereof).

Advice requested by parliament or government	Regarding several legal acts, for instance, Draft Law on Credit Bureau, Draft Law on Debt Retrieval, Amendments to the Schengen Information System Operation Law.
Other relevant general activity information	During the telephone consultation times the main questions asked by the callers: 1. Is certain information considered as personal data? 2. When, who and where can one carry out video surveillance? 3. How to fight against unlawful personal data processing in the internet? 4. Personal data processing within the debt-collection process. 5. How can data subjects exercise their rights for data protection more effectively?
Inspection activities	
Inspections, investigations	Most people who contacted the Data State Inspectorate of Latvia have indicated a possible breach of the Personal Data Protection Law in the following areas (similar to the previous year): 1) personal data processing on the Internet (also in cases when the controller has not foreseen the appropriate technical means for data protection); 2) personal data processing related to debt collection and setting up credit history; 3) identity theft — when the personal data of people are provided, thus unlawful personal data processing is carried out (many cases regarding wrong personal data submitted to State or Local Government Police regarding several administrative violations); 4) data processing carried out by in-house maintenance companies; 5) video surveillance.
Sanction activities	
Sanctions	The sanctions of the Data State Inspectorate are provided within the Latvian Administrative Violations Code.
Penalties	There were fines applied up to LVL 18 910 (~EUR 26 119). The biggest fine was LVL 2 000 (~EUR 2 762) that was applied to a debt collecting company for illegal personal data processing and for not providing the information to a data subject. Two fines were applied regarding personal data processing within SIS.
DPOs	
Figures on DPOs	12 Data protection officers registered.

B. Information on case-law

In 2012 the number of cases increased where the Personal Data Protection Law has been violated and the sanctions for such violations are foreseen with the Criminal Law, thus these cases were forwarded to the office of prosecutor general. Also the number of cases has increased where there was a necessity to cooperate with DPAs of other EU countries in order to carry out the investigation.

LITHUANIA

A: Summary of activities and news

European Data Protection Day was celebrated on 30 January 2012. A press conference and activities at the Seimas of the Republic of Lithuania on Data Protection Day 'Data protection and modern technologies' were organised. On 7 February 2012 Data Protection Day was commemorated at the Vilnius Lyceum. The aim of the day was to give better understanding of threats to personal data security while using modern technologies. The main target group was students of the Lyceum, as well as the general public.

In March 2012 in Estonia the Estonian, Latvian and Lithuanian data protection supervisory authorities met in aim to begin Baltic States cooperation. During the meeting it was decided to carry out joint investigations into the international companies operating in all three countries. Information on planned major activities and the institutions' priorities for 2012 was exchanged and major issues of forthcoming Schengen evaluation and EU data protection reform were discussed. Also a decision was made to organise such meetings annually.

The outcome of this meeting, in the year 2012, joint investigations in all three countries were carried out in hotels belonging to the Radisson Blue international network. The aim of the investigations was to check the legality of the hotel guests' personal data processing for accommodation purposes. During investigations several incompatibilities to personal data protection requirements were established and orders to the hotels were given.

The SDPI together with a joint stock company, Expozona, on 19 May 2012 organised a conference, 'Employees personal data processing and the disclosure of data to third parties — topic issues and problems'. The event was dedicated to the 15th anniversary of the SDPI and was devoted to companies, institutions and organisations, managers, lawyers, professionals responsible for the personal data processing of employees.

On 14 June 2012 the Lithuanian Business Confederation and the SDPI signed a cooperation agreement in aim to achieve a more effective and constructive cooperation between business and public institutions in the protection of personal data. Strengthened co-operation will help to prevent violations of the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter — LLPPD) and to encourage the business community to comply with the rules of personal data protection.

Organisation	State Data Protection Inspectorate
Chair and/or College	Dr Algirdas Kunčinas
Budget	Allocated and executed LTL 2 001 million (EUR 579 530)
Staff	30
General Activity	
Opinions, recommendations	N/A
Notifications	1 258
Prior checks	308
Requests from citizens	15

Complaints from citizens	324
Advice requested by parliament or government	N/A
Other relevant general activity information	4 008 consultations; 103 public information releases; 3 summaries on the preventative investigation results and case-law; 99 conclusions on the EU and the Council of Europe documents; 108 responses to inquiries from parties to the Convention (ETS No 108); 277 coordinated legal acts and data controller documents; 6 prepared legal acts, 4 public consultations.
Inspection activities	
Inspections	45 (data processing legitimacy, scope and data subject rights in Internet shops, public utility enterprises).
Sanction activities	
Sanctions	The SDPI drew up 37 protocols of administrative violations.
Penalties	N/A
DPOs	
Figures on DPOs	N/A.

B. Information on case-law

Processing of personal data related to the heads of legal entities

The SDPI received a complaint in which it was questioned whether the association had the legal grounds to forward information to journalists about complainant's debts to associations, which were published in the newspaper. The SDPI determined that in the newspaper all data referred only to the complainant as a head of the company thus the LLPPD is not applicable. This decision was appealed by the complainant to the Vilnius district administrative court. The Court dismissed the appeal as unfounded, concluding that the data about the company, e. g. the name of company's head, shall be considered as a data of a legal entity. The complainant appealed this decision to the Supreme Administrative Court, which also stated that such data shall be considered as a data of a legal entity, which is open to the public and freely available to all individuals and therefore the LLPPD, which regulates the processing of information relating to a natural person was not violated.

Publication of personal data on the Internet for preventative purposes

The SDPI drew up a protocol of administrative violations to the forester of the forests enterprise (hereinafter — Enterprise), which on the Enterprise website published individuals' personal data (name, surname, full residential address and information about the administrative violation protocol issued to the individual, but not at the time effective) not having any legal ground provided for in Article 5 of the LLPPD or any other criteria for lawful publication of data mentioned. The district court closed administrative violation case without finding the Enterprise guilty. The Court concluded that the data mentioned were published in the legitimate interest of prevention stating that Article 254 of the Administrative Code of the

Republic of Lithuania provides that administrative violation cases shall be made public. In order to increase the educational and preventative role in such cases they can be heard directly at the labour collectives, the administratively liable person's learning place or place of residence.

The Supreme Administrative Court at the request of the SDPI reopened the process and ruled out that in this case disclosure of personal data violated the LLPPD. The court recognised that administrative offences prevention is one of the possible legitimate grounds for personal data processing, however in assessing the balance between the aim of publication and the nature of the personal data published and the completeness of data, as well as the fact that information was published on not-yet-effective protocols and despite the fact that the person appealed to the court protocol in question, continued to be published, a panel of judges decided that in this case the public interest in the prevention of violations did not outweigh a person's right to privacy. The Supreme Administrative Court decided that in these circumstances preventative and educational function could be carried out without such detailed personal data (name, surname and residence address). Especially that place of residence generally is not associated with the administrative offence and has no educational effect, which makes the address excessive. Publication of person's name and surname is making effect only to the person concerned. For the general public preventative and educational impact has information indicating the inevitability of responsibility and the fact that the offense is punishable and what sanctions were applied to the person.

LUXEMBOURG

A. Summary of activities and news

Legislative changes

There were no legislative changes in the field of data protection and privacy in 2012.

Key topics

The CNPD advised the Luxembourgish government by giving opinions on a vast array of laws and regulations on which it was consulted. The main topics in 2012 were:

- the implementation of a national pupil database held by the Ministry of Education;
- the national register of physical persons, the municipal population registers and the electronic identity card;
- the national cancer register;
- the reform of the law concerning criminal records;
- the law on over-indebtedness;
- the introduction of an electronic petition system for the Luxembourgish Parliament.

News

In 2012, the Luxembourgish DPA had to intervene multiple times to control if the law on data protection had been respected. On one occasion, there was an intrusion in a database of the Ministry of Sports containing personal information of over 48 000 people. In another case, the CNPD verified if the retention periods for previously stored photos of citizens had been respected during the replacement of their defective identity cards. In December 2012, the CNPD and the CNIL (France) were invited by the Article 29 Working Party to take the lead in the analysis of the 'Microsoft Services Agreement' and the 'Microsoft Online Privacy Statement'.

Key events and awareness raising

The CNPD organised the Spring Conference of European Data Protection Authorities in Luxembourg from 2-4 May 2012. 138 commissioners from 38 countries and representatives from the European Commission, the Council of Europe and the OECD participated in the conference with the theme: *'The reform of EU Data protection: meeting the expectations?'*. This event was an opportunity to discuss how the modernisation of the EU legal framework shall enhance the privacy of citizens in the digital age and in a globalised world as well as what measures need to be taken to prepare these changes.

Besides this big event, the Luxembourgish DPA participated in multiple awareness-raising events aimed at the general public, like the European Data Protection Day with the slogan *Votre vie privée n'est pas privée de droits (*Your privacy is not deprived of rights*).* 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 WEIMERSKIRCH — Commissioner
Budget	EUR 1 636 000
Staff	College: 3 Legal department: 5 Notifications and Prior checks: 2 General administration: 3 Communication and documentation: 1 IT and logistics: 1 Total: 15
General Activity	
Decisions, opinions, recommendations	438
Notifications	586
Prior checks	423
Requests from data subjects	228
Complaints from data subjects	133
Advice requested by parliament or government	6
Other relevant general activity information	Meetings and consultations (w. public/private sector): 132 Information briefings and conferences: 10 BCR as lead DPA: 2
Inspection Activities	
Inspections, investigations	18
Sanction Activities	
Sanctions	0
Penalties	N/A
DPOs	
Figures on DPOs	Designated DPOs during 2012: 11 Total of designated DPOs (at date of report): 47

B. Information on case-law

The District Court of Luxembourg, 13th correctional chamber (1 February 2012, No 534/2012) on the validity of proof (video-surveillance images) collected in absence of a prior authorisation by the CNPD.

This case pertained to a hit-and-run accident in a tunnel, recorded on CCTV cameras for which no prior authorisation had been requested. The defence lawyer of the accused pleaded *'in limine litis'* that the videotapes of the accident were to be discarded as proof, considering that no prior authorisation from the CNPD had been obtained.

The Court ruled that the images are, nevertheless, to be allowed as means of proof. To conclude in this manner, the Court operates an analysis of the legitimacy conditions of said surveillance and clearly refers to the purpose test, as set out in the Luxembourgish law on data protection.

Contrary to the case reported on during 2009 (District Court of Luxembourg, 9th correctional chamber, No 387/2009) which the CNPD deemed highly prejudicial, as it was based on vague judicial concepts of the judge's intimate conviction, this new case introduces a more transparent and correct way of analysing the validity of proof in absence of a prior authorisation by the CNPD.

MALTA

A: Summary of activities and news:

During the year under review, no legislative interventions were made to the Data Protection Act. However, a legal notice was in the process of being drafted establishing 1 January 2013 as the date when all the provisions of Legal Notice 239 of 2011 were to come into force. This regulation transposes the amended ePrivacy Directive 2009/136/EC 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. This Office initiated the process of developing ad-hoc guidelines to provide data controllers with the necessary direction concerning the implementation of the cookie consent requirement.

The Freedom of Information Act (Chapter 496 of the Laws of Malta) was enacted by Parliament in 2008. The purpose of the Act is to establish the right to information held by public authorities with a view to promoting added transparency and accountability in government. The Act was brought fully into force on 1 September 2012 and vested the Commissioner with the additional responsibilities, inter alia, to receive and decide on applications for a review of decisions by public authorities, to serve enforcement notices on public authorities to comply with his decisions and to promote the observance of the Act. During the period under review, the Commissioner received three complaints, two were against the Malta Police Force and one was against the Permanent Secretariat of the Ministry for Home Affairs.

This Office sustained the efforts to meet the various sectors with the objective to discuss data protection issues and provide the necessary guidance. Meetings were held with the two main credit referencing agencies on the island and, after a series of discussions, guidelines were formulated and adopted to promote good practice in the processing of individuals' personal data by credit institutions.

During 2012, four persons felt aggrieved by the decision of the Commissioner and lodged an appeal before the Information and Data Protection Appeals Tribunal. Whereas one appeal was withdrawn by the appellant following the first sitting of the Tribunal, the proceedings of the second appeal were still ongoing by year end and, in the other two cases the Chairman of the Tribunal found in favour of the Commissioner and dismissed the appeals. These decisions were considered to be final and conclusive given that no party appealed such decisions before the Court of Appeal within the thirty-day window established by law.

Following the first evaluation which was carried out by the Schengen Evaluation Data Protection Committee in 2006 as part of Malta's preparations to accession to the Schengen area, in July this Office was subjected to the second peer review by the same evaluation committee. Experts called at the Office to evaluate the internal operations and procedures, in particular the exercise of the Commissioner's supervisory role. Presentations by the Commissioner, technical staff and the data protection officer within the Ministry of Foreign Affairs were made. The outcome of the evaluation was presented to the Schengen Working Party during the Council meeting where it was concluded that this Office was adequately geared to exercise the role of data protection regulator on all data controllers including the Police. A minimal number of recommendations were also made and this Office took immediate action to address them.

On 28 January, this Office joined other Data Protection authorities across Europe 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.

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 strong and effective way to increase awareness with the public at large.

Organisation	Office of the Information and Data Protection Commissioner
Chair and/or College	Information and Data Protection Commissioner
Budget	ca. EUR 300 000
Staff	Commissioner - 1 Professional Staff - 3 Technical Support - 2 Administrative Support - 3
General Activity	
Decisions, opinions, recommendations,	48 decisions were issued in relation to complaints received by the Commissioner 23 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	228 new notifications were received
Prior checks	5 prior checking requests were received
Requests from data subjects	Queries received by phone - an average of 10 daily calls Queries received by e-mail - 156
Complaints from data subjects	72 complaints
Advice requested by parliament or government	N/A
Other relevant general activity information	N/A
Inspection activities	
Inspections, investigations	8 inspections were carried out relating to investigations of complaints received from data subjects and routine inspections on

	Police systems, specifically on SIS and Europol.
Sanction activities	
Sanctions	Official reprimands were issued to data controllers. No legal proceedings were initiated before the Courts of Law.
Penalties	No financial penalties were imposed to data controllers.
DPOs	
Figures on DPOs	12 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 we receive from various sources in society via different means, such as phone calls, e-mails 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 2012 were among others: profiling, adequate protection of medical data and data security.

One of the major investigations carried out in 2012 dealt with profiling by a large supermarket chain in the Netherlands. Public statements from the retailer revealed plans to provide customers with personalised offers based on an analysis of their purchase history. To this end, the supermarket chain would use the information collected for all purchases made while using the customer loyalty card. After an investigation, the Dutch DPA concluded the consent the retailer requested from its customers was invalid, amongst others because of a lack of information on the data collection and subsequent analyses that would take place. As a result of the investigation, the retailer has decided to postpone the launch of the personalised offer programme. In the meantime, it has updated its privacy policy and general conditions, after which it will again ask for consent from its customers.

Another investigation that was carried out in 2012 followed public uproar about a television programme intended to show the ins and outs of the Accident and Emergency Department of a large hospital in Amsterdam. For the programme, both patients and staff were filmed during the time they spent in the A&E Department. Once the television crew had assessed the 'case' of the patient was interesting enough to be broadcast, he or she was asked for permission to use the camera footage for the broadcast and to make further recordings. Considering the location of the recordings — a hospital — mostly medical data would be discussed in the footage, requiring special attention. The Dutch DPA concluded that the required consent had not been legally obtained by the television crew for various reasons. In the first place, consent was not obtained before the start of the data processing, since recordings were made from the moment patients and crew entered the A&E Department. Furthermore, the information provided was insufficient for the patients to make a fully informed decision. Finally, given that the patients entering an A&E Department in general would be in a situation of distress, their dependency on the services of the hospital would be such that in the view of the Dutch DPA consent — even if fully informed — could never be freely given.

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. In 2012, advice was issued on the proposal to allow for an additional rent increase for households with a mid-level income (between EUR 33 000 and 43 000 per year). For these tenants, an annual rent increase of inflation plus one per cent would be applicable. To assess which tenants would be liable to such a rent increase, the Tax Authority would transfer information on the income category of the tenant to the landlord. The Dutch DPA advised that the proposal in its eyes was not sufficiently motivated and did not fulfil the requirements of proportionality and subsidiarity. It had not been demonstrated by the Government to what extent this infringement of the fundamental right to data protection would contribute to a better availability of rental property (the identified purpose of the bill) and why alternative, less intrusive means could not be used to get a similar result.

Organisation	Dutch Data Protection Authority
Chair and/or College	Jacob Kohnstamm — Chair Wilbert Tomesen — Commissioner and Vice-Chair Madeleine McLaggan-Van Roon — Commissioner* Mrs McLaggan has been exempted from her tasks as Commissioner of the Dutch DPA during the time she is preparing a scientific report on the relations between competition law and data protection upon request of the Secretary of State for Security and Justice.
Budget	Allocated: EUR 7 679 000- Executed: EUR 7 746 000
Staff	75.8 FTE
General Activity	
Decisions, opinions, recommendations	213 (investigations, guidelines, code of conduct, prior checks, sanctions and advice in legislative process)
Notifications	5 966
Prior checks	93
Signals ([12]) from data subjects	6 042
Advice requested by parliament or government	42
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	58
Sanction Activities	
Sanctions	12
Penalties	n/a
DPOs	
Figures on DPOs	345 ([13])

([12]) Since April 2011 all citizen contacts are registered as a signal. These signals are used to prioritise our tasks. Therefore, it is not registered by which means signals are received by the DPA, but to which sector they are subjected.

([13]) Number correct as of September 2013.

B. Information on case-law

During the year of this report, several data protection-related cases were dealt with by the courts in the Netherlands. Notably, in one of the cases the Amsterdam court held that a book could be considered to be a file in the sense of the data protection legislation, if a register of persons is included. In a case related to the amount of rent due for certain types of housing, the court in The Hague decided that the Dutch Data Protection Act needs to be fully read in conjunction with Article 8 ECHR, the right to privacy. Proportionality and subsidiarity need to be considered at all times, also in relation to the purpose of the proposed measure, and cannot be ignored by a ministerial decision.

In one case during 2012, a decision of the Dutch DPA was the subject of a procedure before the Rotterdam court. The borough Charlois in the municipality of Rotterdam had introduced an obligatory registration of the country of birth in order to implement so-called preferential treatment to offer assistance for kids having several problems (arrears at school, early criminal tendencies, maltreatment, etc.).[14] Given that most kids with problems are from a non-native Dutch background, the borough considered it useful to be able to screen possible problematic situations by taking into account the country of birth. The Dutch DPA held however this would come down to racial profiling, and thus processing of sensitive data. Since no legal basis for such processing was available, the Dutch DPA order the borough to stop the registration of the country of birth, with a conditional fine of EUR 2 000 per day if the processing continued. The borough seized the court, but lost the procedure. In the meantime, the contentious processing has been stopped.

(14) Also see the 15th Annual Report covering 2011.

POLAND

A. Summary of activities and news

The Act on exchange of information between law enforcement authorities of the Member States of the European Union (Journal of Laws of 2011 No 230 item 1371) came into force on 1 January 2012. This Act implemented partially Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters into Polish legal framework and at the same time it changed some provisions of the Act on the Protection of Personal Data.

As a result of derogation as of 1 January 2012 of Article 7a (2) of the Act of 19 November 1999. The Business Activity Law (Journal of Laws of 1999 No 101, item 1178), which excluded personal data contained in the register of business activity from the application of the provisions of the Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2002 No 101, item 926 with amendments), hereinafter referred to as the Act, currently, personal data of natural persons, regardless of the fact whether they conduct business activity or not, are subject to the protection provided for in the Act.

In 2012 the Administrative Execution Team started its work. This new organisational unit in the GIODO Bureau was established by GIODO as a result of amendment to the Act on Personal Data Protection which entered into force on 7 March 2011 and granted the Inspector General for Personal Data Protection (GIODO) the powers of an enforcement authority in the scope of administrative enforcement of non-pecuniary obligations (Article 12, (3)).

On 15-17 April 2012 the 2nd Evaluation Mission was conducted in Poland aimed at evaluation of the level of implementation of the Schengen Acquis. In the Mission Report the EC emphasised GIODO's significant achievements in the education and information field and highly rated the legal tools for data protection in Poland and GIODO's competence in performing supervision and monitoring over personal data processing in Poland.

GIODO continued its involvement in the works related to the EU data protection framework reform. The most important events and activities in this regard included:

1. The Inspector General attended a Meeting of the Commission of Justice and Human Rights in the Seym (16 February 2012) and Senate (lower and upper chamber of the Polish Parliament) during which he presented to Members of the Parliament the basic objectives of the EU data protection reform.
2. On 7 March 2012, the Inspector General for Personal Data Protection, the National School of Public Administration (KSAP) and European Commission Representation in Poland organised at the KSAP seat in Warsaw a Conference on 'Reform of Personal Data Protection Rules in the European Union. Preliminary assessment of its scope and consequences'. The Conference launched a comprehensive discussion on the plans to shape a new privacy and data protection model in the European Union.
3. In connection with the EU data protection reform, the Inspector General is involved in consultations with various sectors. He has so far attended consultation meetings with the following sectors and institutions:
   - banking sector;
   - Polish Insurance Association;
   - Polish Trade and Distribution Organisation;

- representatives of telecommunications and IT sector associated in the Polish Chamber of Information Technology and Telecommunications;
- National Council of the Judiciary;
- and others.

4. GIODO participated in the Interparliamentary Committee Meeting devoted to 'The reform of the EU Data Protection framework - Building trust in a digital and global world' held on 9-10 October 2012 in the European Parliament in Brussels. The Interparliamentary Committee Meeting was prepared jointly by the EP Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Legislative Dialogue Unit (LDU) was intended to reflect on the most important issues and to engage members of the European Parliament and national Parliaments in an exchange of views and a constructive dialogue.
5. Meeting between GIODO and Assistant European Data Protection Supervisor took place on 12 December 2012, at which GIODO along with representatives of government administration discussed the issues of the EU data protection reform and its impact on national law.

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 15 060 000
Staff	126
General Activity	
Decisions, opinions, recommendations	1297 decisions issued (427 decisions related to registration proceedings, 53 were issued in connection with conducted inspections, 762 were issued as a result of proceeding initiated by a complaint, and 51 concerned authorisation to data transfer to a third country). 126 addresses and requests were addressed to state authorities, territorial self-government authorities, as well as to state and municipal organisational units, private entities performing public tasks, natural and legal persons, organisational units without legal personality and other entities in order to ensure efficient protection of personal data
Notifications	16 267 personal data filing systems registered.
Prior checks	As a result of registration procedures (prior checking) 3 359 personal data filing systems containing sensitive data were entered in the register of personal data filing systems; processing of personal data filing systems containing sensitive data can start only after completion of the registration procedure. In connection with implementation of National Components of the VIS System inspections regarding the National Information System

	(KSI) at the General Police Headquarters were conducted, pursuant to the Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System.
Requests from data subjects	4 208 legal questions were sent to the Polish DPA. 11 001 explanations were also provided through GIODO's information hotline.
Complaints from data subjects	Complaints concerning infringement on personal data protection, including: public administration (88 complaints), courts, public prosecutor's office, the Police, bailiffs (44 complaints), banks and other financial institutions (129 complaints), Internet (84 complaints), marketing (28 complaints), housing-related (56 complaints), social, property and personal insurance (12 complaints), Schengen Information System (12 complaints), telecommunications (40 complaints), employment (11 complaints), other (386 complaints).
Advice requested by parliament or government	Opinions were expressed on 598 draft acts submitted for review to GIODO.
Other relevant general activity information	66 - number of training courses conducted by GIODO concerning provisions on personal data protection, especially for public institutions. 207 education establishments, including primary, middle and secondary schools, and teacher vocational training centres, participated in the 3rd edition of the Poland-wide programme 'Your data, your concern. Educational initiative addressed to students and teachers' for the academic year 2012/2013.
Inspection Activities	
Inspections, investigations	165 inspections, including: - 17 inspections concerning personal data processing in the National Information System enabling public administration authorities and justice authorities to use data collected in SIS and VIS; - 9 inspections in cooperative banks and 2 in banks associated with cooperative banks; - 5 inspections at public telecommunications network operators',

	publicly available telecommunications services providers; - 8 inspections in bone marrow donor centres; - 10 inspections of the Higher Education Information System; - 11 inspections at entities' running hotels.
Sanction Activities	
Sanctions	GIODO keeps no general statistics on sanctions. However, for example in connection with GIODO's powers of an enforcement authority, 99 administrative proceedings were instituted within execution of GIODO's decisions. Whereas in connection with inspections conducted in 2012, GIODO instigated 46 administrative proceedings against data controllers and issued 23 decisions which included an order to restore a proper legal state. Also, GIODO issued 64 decisions on refusal to register a data filing system. No sanctions imposed by the DPA in the reporting period.
Penalties	No fines were imposed in 2012.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In 2012 in cases considered by GIODO 73 judgments were issued by the Supreme Administrative Court and the Voivodeship Administrative Court. The following judgments are noteworthy.

I. Judgment (Ref. No II SA/WA 2333/11) by the Voivodeship Administrative Court in Warsaw

The Court confirmed GIODO's negative standpoint on the case in which a Company demanded from a Trade Union operating at that Company to disclose a list of names of its members for the purpose of verification of specific rights of Board Members of that Union. The Court emphasised that giving the number of trade union's members would be sufficient for such verification, and collection of sensitive data, i.e. data on union membership, for such purpose by the employer, had no legal basis in Article 27 (1) of the Act on Personal Data Protection, whereby specific provisions such as the Act on Trade Unions or the Labour Code also did not provide such legal basis. At the same time, in the Court's view such demand to disclose a list of names of all members violated the purpose limitation, necessity and proportionality principles.

II. Judgment (Ref. No II SA/WA 2367/11) by the Voivodeship Administrative Court in Warsaw

The Court agreed with the assessment carried out by GIODO in the case concerning the processing of personal data in connection with assignment of claims, which arose at the time when the complainant conducted business activity and was directly related to that activity. In the Court's opinion, the data protection authority is not competent to assess the correctness of civil-law contracts and arising

disputes, in particular to assess whether the assignment of claims agreement is admissible, effective or valid, as only common courts have material jurisdiction in this respect. Whereas, from the perspective of personal data protection principles disclosure of personal data in connection with assignment of claims did not violate the provisions of the Act on Personal Data Protection.

III. Judgment (Ref. No II SA/WA 2848/11) by the Voivodeship Administrative Court in Warsaw

The Court confirmed the DPA's opinion, according to which disclosure by a Company of invoices containing a complainant's personal data to the Regional Court for the purposes of civil proceedings and to the Police Headquarters for the purposes of conducted criminal proceedings had legal basis in Art. 23 (1) points 2 and 5 of the Act on Personal Data Protection, i.e. if it is necessary for the purpose of exercise of rights and duties resulting from a legal provision, and if processing is necessary for the purpose of the legitimate interests pursued by the controllers. Moreover, the Court referring to established case-law of administrative courts confirmed that GIODO is not competent to control procedural acts in criminal or civil proceedings undertaken by competent authority, including evidence proceedings with the use of personal data.

C. Other important information

In the reporting period the increasing trend in the number of registered personal data filings systems as compared to previous years (in 2010 — 9 921, in 2011 — 11 845, in 2012 — 16 267) continued. Moreover, growth (as compared to 2011 by 40 %, to 2010 — by 164 %, and to 2009 — by as much as 184 %) in the number of files notified to registration was observed. In 2012 GIODO handled 4 090 updating notifications submitted by data controllers, whereby GIODO issued 287 decisions on removal of a data filing system from the Poland-wide open register of personal data filing systems.

On the occasion of the European Data Protection Day, on 30 January 2012 the Inspector General traditionally organised an Open Day for all citizens at the seat of his Bureau, and Conference entitled 'What does the State know about its citizens? The principles of data processing in public registers'. Also, as usual European Data Protection Day was celebrated in Brussels.

In connection with the great interest of the public in Open Days organised on the occasion of Data Protection Day in January in its seat in Warsaw, GIODO has undertaken a new initiative consisting of organising such events also on other dates in other cities all around Poland. In 2012 additional open days were organised in other Polish cities — on 22 November in Dąbrowa Górnicza and on 23 November in Cracow.

On 23-24 April 2012, the 51st Meeting of the International Working Group on Data Protection in Telecommunications (the so-called Berlin Group) was organised by GIODO in Sopot, Poland. It concentrated on data processing in cloud computing solutions, the execution of the right to be forgotten and the profiling of Internet users by marketing companies using special analysis tools. A big achievement of the meeting was the adoption of a working document comprising the common position of the Group on the principles of privacy protection in case of data processing with the use of cloud computing, called the Sopot Memorandum.

The Leonardo da Vinci partnership project 2012, 'Raising awareness of the data protection issues among the employees working in the EU' was launched in 2012. The project is aimed at providing educational materials to natural persons undertaking employment in one of the countries participating in the project. The project partners, i.e. Data Protection Authorities from Poland, Czech Republic, Croatia and Bulgaria, are involved in works on a publication which will focus on providing the natural persons employed or planning to be employed in one of the countries participating in the project with guidance and advice on personal data protection and privacy.

Moreover, it is worth noting that the 'Code of good practice as regards the protection of customers and potential customers' personal data' was developed by the Polish Automotive Industry Association in cooperation with GIODO. The document constitutes an integral part of an agreement on cooperation between both institutions concluded on 16 November 2012.

PORTUGAL

A. Summary of activities and news

During 2012, the DPA consolidated its dematerialisation internal procedures, increasing the possibilities of electronic notification of data processing and shortening the response time to data controllers.

On the other hand, the DPA increased its inspective action, either following complaints from data subjects or on its own initiative. Video surveillance, unsolicited electronic communications for marketing purposes and employees' monitoring at the workplace (e.g. GPS devices in cars) were the most significant subjects of the complaints received.

The DPA kept closely monitoring the developments of e-Government projects by public bodies, in particular in the health sector and in the police sector, and had a continuous intervention in the legislative process by issuing almost 100 opinions on draft law affecting data protection.

The DPA also promoted meetings with stakeholders concerning the implementation of the new rules of the e-Privacy Directive and regarding the use of GPS in the employment context.

In what concerns awareness-raising activity, it should be underlined that the efforts put forward by the DPA, since 2007, by developing a dedicated and structured project addressed at children in schools — the DADUS Project — resulted in upper-level support by the Government. In 2012, the Ministry of Education formally introduced in the ICT discipline curricular goals data protection and privacy issues. This discipline is common to all pupils in 7th and 8th grade, involving children from 12-14 years old. Therefore, the DADUS Project is being reviewed accordingly in order to better suit this new reality, where the DPA will play a more supportive role instead of taking the lead.

Organisation	National Commission of Data Protection
Chair and/or College	Colleagiate body composed of 7 members: Filipa Calvão (President), Luís Barroso, Ana Roque, Carlos Campos Lobo, Helena Delgado António, Vasco Almeida, Luís Paiva de Andrade
Budget	Initial Budget allocated: EUR 2 324 352,00 State Budget: EUR 1 193 885 DPA own receipts: EUR 1 130 467 (actually received: EUR 1 556 838) Budget executed: EUR 1 445 188.45
Staff	25
General Activity	
Decisions, opinions, recommendations	12 006 binding decisions (including 10 083 authorisations for data processing, deliberations on infraction procedures and deliberations on requests of access to data by third parties, Schengen right of access and elimination and others)
Notifications	11 306

Prior checks	10 325
Requests from data subjects	Figures not available (the Front Office handles requests from data subjects and data controllers)
Complaints from data subjects	588 (formal proceedings opened)
Advice requested by parliament or government	90 prior opinions on draft law containing data protection dispositions
Other relevant general activity information	13 504 new proceedings (notifications, complaints, opinions, infractions, access by third parties and others); 130 requests concerning the exercise of the right of access and deletion to the Schengen Information System (indirect access through the DPA); 684 requests for opinions from telecom providers concerning the lifting of the confidentiality of the caller in case of disturbing calls.
Inspection Activities	
Inspections, investigations	1 005 investigations started (infraction proceedings), including the performance of 359 inspections on the spot
Sanction Activities	
Sanctions	169 fines applied by the DPA
Penalties	± EUR 283 000
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 (approx. EUR 751 131)
Staff	42 plus the President and the Vice-president of the authority)
General Activity	
Decisions, opinions, recommendations	834 out of which 2 normative decisions
Notifications	10 014
Prior checks	-
Requests from data subjects	59
Complaints from data subjects	667
Advice requested by parliament or government	51
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	131 on the spot and 41 in writing
Sanction Activities	
Sanctions	24 fines with a total amount of RON 36 000 (approx. EUR 8 115)
Penalties	84 warnings
DPOs	
Figures on DPOs	-

B. Information on case-law

Case-law 1

Based on several notices addressed by a petitioner, the data protection authority carried out a series of investigations to a data telephone and Internet service provider controller.

The purpose of the inspections consisted in the verification of the way in which the processing was carried out of the traffic data of the subscribers/users of Internet services of the controller, particularly, concerning the activation, unsubscription and the functioning of MyClicknet service.

Following several investigations it was ascertained that the MyClicknet service, operated by the data controller since September 2011, represents a service with value added, whose purpose is the customisation of the navigation on the Internet of its subscribers/users, with the view of providing behavioural advertising and supposes directing a copy of the traffic in order to analyse and process the traffic data, before and after accepting this service, by installing cookies on the computers of its subscribers/users. This service was implemented by using the Phorm solution and installing the Phorm equipment on the data controller's network.

The above-mentioned operations had to be carried out by observing the provisions of Articles 4 and 5 of Law No 506/2004.

In this respect, the data protection authority solicited for the data controller to present the proof for obtaining in advance the informed consent (in writing) of the subscribers/users for the processing of their traffic data, in the meaning of the provisions of Law No 506/2004 for this purpose specific for providing the invitation page, a page which later allows the installation of the cookies related to the MyClicknet service.

In regard to this request, the representatives of the data controller could not present such proof, the document invoked by these (general conditions for providing the data controller's services) did not contain such clauses which could be assimilated to an expressed and informed consent for this specific purpose.

At the same time, the data controller did not present proof for obtaining the informed consent of the subscribers/users to opt-out of the cookies installed, previously and after providing the invitation page. Thus, by previously providing the invitation page, the system permits the verification by comparing the attempts of the subscriber/user to access the Internet, with the URL addresses from the predefined list implemented in the system.

Following the investigations performed, the contravention sanction of the provider was disposed, by applying a fine for the following:

1. the non-compliance with the provisions of Article 4 paragraph (2) of Law No 506./2004, because the data controller carried out operations of directing and supervising the communications and the related traffic data of its subscribers/users with the meaning of providing the value added by the MyClicknet service, before providing the invitation page, under the aspect of performing a copy of the traffic through the mirroring process, of verification by comparing the attempts of the subscriber/user to access the Internet, with the URL addresses from the predefined list implemented in the system and of verification of the existence of a cookie oix specific for this service, without fulfilling any of the conditions stipulated in Article 4 paragraph (2) letters a)-c) from Law No 506/2004;
2. the non-compliance of the conditions provided by Article 4 paragraph (5) of Law No 506/2004 and of Article 5 of Law No 506/2004 concerning the processing of traffic data, because the data controller processed the traffic data of its subscribers/users to Internet services with the purpose of providing the value added MyClicknet service which implies the usage of the

electronic communication network in order to store the information in its terminal equipment and to obtain access to the information stored in this manner (by installing cookies), without previously obtaining the expressed and informed consent of the subscribers to the Internet services of the data controller, before providing the invitation page which allows the expression of the consent or of the disagreement for the activation of the MyClicknet services, and after for the installation for the opt-out cookie for those who did not give their consent.

Case-law 2

More petitioners complained about the dissemination of the Internet pages of several courts of justice (available through portal.just.ro) of certain personal data than the ones necessary for ensuring the publicity of the causes on their role. Following the investigations carried out by the data protection authority, non-compliance was ascertained with the provisions of Law No 677/2001 and, thus, recommendations for the Ministry of Justice and the Superior Council of Magistracy concerning the way of functioning the ECRIS application used by the courts of justice:

a) the exact determination of the personal data which are strictly necessary for the accomplishment of the purpose of ECRIS application, meaning the portal of the courts of justice under the conditions in which the data must be adequate, pertinent and not excessive (posting only the name and surname of the justice seekers within the published solution);

b) the elaboration, at central level, of unitary instructions referring to the processing of personal data, which are applicable to all the persons being under the authority of the data controller, as users of ECRIS application;

c) the training of the persons (employees) who work under the authority of the data controllers concerning the dispositions of Law No 677/2001, modified and completed, especially regarding the processing of personal data within the ECRIS application, the portal of the courts of justice;

d) the review of all the registrations made so far in the ECRIS application, according to the above-mentioned recommendations, as well as the deletion of the personal data which do not respect the legitimacy conditions of processing the personal data;

e) the set-up of a limited period of storage of personal data contained in the ECRIS application, the portal of the courts of justice, related to the proportionality principle of the processing performed and in compliance with the legal provisions of the Code of civil procedure, the Code of criminal procedure and of the Law of National Archives;

f) the adequate protection of the personal data against the accidental or illegal destruction, loss, alteration, disclosure or unauthorised access.

The complaints received were favourably solved, the excessive personal data published by the courts of justice being deleted.

Case-law 3

Following the inspections carried out into several data controllers, as a consequence of receiving several notices, it was ascertained that the accomplishment of the declared purpose of the data processing, meaning to record the working hours of the employees of some group companies, could be fulfilled by alternative methods, less intrusive than the processing of biometrics. So, before introducing this system, the prominence of the work time was performed by signing a presence register and, temporarily, by using access cards. Moreover, after introducing the new system for electronic record of the working hours by collecting biometrics, the record of the working hours for certain employees was still carried out by signing the presence register.

In this context, the data controllers verified were sanctioned with a fine for committing contraventions provided by Article 31 and Article 32 of Law No 677/2001. Also, by decision of the president of the Data

Protection Authority it was disposed to cease in the biometrics processing on the data controllers' employees in order to record the working hours, and the deletion of the biometrics already collected.

Further, there was a follow-up investigation following a new notice from the petitioner stating that the data controllers did not comply with the measures provided by the data protection authority, an inspection of the declarations of the petitioner was not confirmed.

C. Other important information

Regarding the legislative proposals transmitted to the data protection authority, we mention that there were several negative opinions because there was not a correlation of the proposed dispositions with the constitutional principles and regulations, with European Union's legal acts, with the treaties to which Romania is a party or with the framework legislation, as well as the generation of redundancy in statutory.

All these aspects made impossible the issuance of a favourable opinion, the data protection authority proposing the reconsideration and reformulation of draft normative acts.

Of the regulations to which the data protection authority has issued negative opinions, we exemplify:

- a draft law on the retention of data generated or processed by providers of publicly available electronic communication or public communication networks;
- a legislative proposal concerning the collection and storage of data necessary to identify the electronic communications services clients provided through prepaid cards.

Processing of personal data of pre-paid card users

The National Supervisory Authority for Personal Data Processing has given a negative opinion with regard to a legislative proposal on the collection and storage of the data necessary for the identification of customers of electronic communication services provided via pre-paid cards. The provisions of this legislative proposal came into contradiction with the principles established by Council of Europe's Convention 108, as well as with the provisions of Directive 95/46/EC, Directive 2006/24/EC and Directive 2009/136/EC on universal service and users' rights relating to electronic communications networks and services.

Moreover, the legislative proposal infringed on the individuals' right to private life (established under Article 26 of Romania's Constitution, as republished). The processing of the Personal Identification Number (CNP) may be carried out in accordance with the conditions provided by Article 8 of Law No 677/2001 and these of Decision 132/2011; however, as the legislative proposal was drafted it brought serious infringements to the principles of proportionality and storage of data as provided by Directive 95/46/EC and Law No 677/2001.

By establishing the obligation to communicate the identification data upon the data subjects that had already acquired a service of any type from the providers of the electronic communication service, prior to the entry into force of the proposed act, the supervisory authority considered that it infringes on the principle of non-retroactive laws, established under Article 15 paragraph (2) of Romania's Constitution.

The legislative proposal mentioned above also brought infringements upon the consumers' right to make decisions with regard to acquiring pre-paid communication services, as, by imposing the obligation for identification, that might influence the consumer's option with regard to acquiring the service or not.

SLOVAKIA

A. Summary of activities and news

The year 2012 can be described as a year of changes and successful legislative proposals. Based on the Plan of Legislative Tasks of the Government of the Slovak Republic for the second half of the year 2012 the Office for Personal Data Protection of the Slovak Republic (hereinafter the Office) has prepared the whole new draft of the Act on personal data protection.

The objective of changing the act was to completely transpose the Directive of the European Parliament and the European Council 95/46/EC and implement the conclusions and recommendations of the Schengen evaluation in the Slovak Republic in the personal data protection area and law analysis from application practice point of view.

Starting in January 2012 the Office introduced so-called weekly services of monitoring and assessment of materials included in the legislative process within the inter-ministerial review proceeding. The aim of such process is to continuously track all materials included in the inter-ministerial review proceeding and therefore to effectively evaluate and comment on such materials. For any proposed material the Office assessed compliance with the Act on personal data protection to ascertain the legally protected basic requirements of social life while minimising interferences on the right to privacy and the privacy of individuals. For this purpose every legislation draft that governs by its content processing of personal data must comply with the basic requirements that the Act on personal data protection requires.

Nationwide inspections activities of the Office

During the year 2012 the Office carried out several nationwide inspection operations based on the annual plan of control activities. During the planning of the annual plan of control activities the Office focused on the control of personal data processed by the collectors and processors in filling systems which reflected the development of social relations and legislation on protection of personal data.

Copying of official documents in the application for a tax bonus

In 2012 the Office investigated the lawfulness of the personal data processing for the purposes of proof of tax bonus under the Act on income in the four selected tax offices in Slovak Republic. During the investigation the Office found that the tax authorities obtained personal data in order to establish a tax bonus, copying and storing official documents of natural persons. However the Act on Income Tax at the time of the inspection activity did not allow copying and storage of official documents for this purpose with the result that the procedure of the tax authorities was in violation of Section 10 Paragraph 6 of the Act on personal data protection No 428/2002 Coll.

Processing of personal data by real estate agencies

In 2012 four real estate agencies were subject to inspection activity by the Office. The aim of the inspection was to review the activities of the real estate agencies as the controllers processing personal data for the purpose of concluding lease contracts, or for the purpose of concluding purchase contracts for the property and the related entry on the Cadastre and Registration of Ownership. During the inspection the Office found that the controllers obtained some of data subject's personal data by copying official documents. Such personal data collection was not necessary to achieve the purpose of their processing under the Section 6 Paragraph 1 Point (d) in connection with Section 10 Paragraph 6 of Act No 428/2002 Coll.

Processing of personal data by orphanages

In 2012 the Office investigated the status of personal data protection processed under Act No 305/2005 Coll. on Socio-Legal Child Protection and on Social Custody and on the changing and amending of other

acts, as amended in five chosen orphanages as the controllers on the territory of the Slovak Republic. Inspection activities especially revealed errors in filing systems and in the instruction of entitled persons.

Processing of personal data by accommodation facilities

In year 2012 the Office also focused on inspecting the processing of personal data by accommodation facilities under Act No 253/1998 Coll. on Notification of Residency of Slovak Republic Citizens and the Population Register in the Slovak Republic as amended, and Act No 404/2001 Coll. on Residency of Foreigners as amended. Control activities were carried out by the Office in five selected controllers.

Processing of personal data by travel agencies

Under supervision of personal data protection during the control activities in 2012 the Office also focused on the processing of personal data by travel agencies as the controllers of filing systems. The purpose of the inspection activities was to review the status of personal data protection and compliance of terms of their processing in particular for the purposes of concluding the trip contracts. Compliance with the administrative procedures the Office verified at five controllers. Control activity has demonstrated that during the contracting period two legal bases for the processing of personal data occurred — the data subject's consent and the necessity of personal data for the performance of a contract to which the data subject is party under the Section 7 Paragraph 4 Point b) under Act No 428/2002 Coll.

Cross-border Personal Data Flow

In 2012 the Office issued twenty-five approvals of cross-border personal data flows to countries that did not provide an adequate level of data protection. Agreement with the cross-border transfer of personal data to the third countries was demanded mostly by controllers established in the Slovak Republic who mostly belonged to multinational holding companies. Personal data were related mostly to the employees, clients and business partners of the controllers.

International Cooperation

Tasks at the international level resulted mainly from the membership of the European Union and in working groups established under auspice and from legal acts of the European Communities.

In spring 2012 the Office held a working meeting at the request of the Serbian Office of the Plenipotentiary for the protection of personal data and information of public importance. This meeting was organised in collaboration with the Centre to share experiences of integration and reform of the Slovak Agency for International Development Cooperation at the Ministry of Foreign and European Affairs of the Slovak Republic.

The subject of the meeting was to provide expert consultation on selected topics in the processing of personal data in the Slovak Republic for the purposes of direct marketing, processing of personal data in electronic media, publication of personal data by controllers in the judiciary, local government, media, processing of special categories of personal data and foreign agenda provided by the Office. The consultations were supplemented by examples from the Office's practice.

Organisation	Office for the Personal Data Protection of the Slovak Republic
Chair and/or College	JUDr. Eleonóra Kročianová
Budget	EUR 876 324
Staff	34 employees

General Activity	
Decisions, opinions, recommendations	
Notifications	200
Prior checks	0
Requests from data subjects	In the evaluated period of time the Office investigated 5 requests from data subjects who exercised their right under the Section 20 under Act No 428/2002 Coll. right to information about the status of the processing of their personal data and information about the source from which the processor obtained their personal data. The processor is obliged to meet the requirements of data subjects and to inform them in written form about the status of the processing of their personal data. In all cases the investigation of the Office proved that the notifications of data subjects were legitimate and thus the processors breached their legal obligation.
Complaints from data subjects	In the evaluated period of time the Office received 200 notifications from natural persons who claimed protection of their rights and law protected interests. The Office also received 52 notifications from other subjects about suspicions regarding the violation of the Act on Protection of personal Data. In the evaluated period of time the Office investigated 321 notifications and suggestions and led 69 proceedings on its own initiative. These proceedings were aimed at subjects in the private sector and also in the public sector. To remedy the founded deficiencies, the Office issued 131 measures in total. From a total of 252 investigated notifications and suggestions about the violation of the Act No 428/2002 Coll, 4 notifiers have exercised the right to file the notice within the legal period of 30 days. In 3 cases the Office postponed the repeated notice in accordance with the Act because of the lack of new facts.
Advice requested by parliament or government	
Other relevant general activity information	The main priority in 2012 was the change in the leadership of the Office and therefore the related subsequent consolidation of employee's establishment. Another priority of the Office was the implementation of the Schengen acquis. Last but not least was the legislative work on the new Act for Personal Data Protection.
Inspection Activities	
Inspections, investigations	In the evaluated period of time the Office carried out 112 inspections in total. Control activities of the Office were realised based on the annual plan of the control activities of the Office.

	During the planning of the control activities the Office aimed at the actual status of processing of personal data by the controllers and processors, their entitled persons and at compliance of processing of personal data with generally binding legal regulations and international documents which the Slovak Republic is bound. The areas in focus by the Office reflected the actual and practical situation about the protection of personal data and potential problems with applications of Act No 428/2002 Coll. and another special Acts. The Office observed increased occurrences of problems during the processing of personal data in the evaluated period of time. These problems were related with the operation of camera filing systems mostly by the natural persons. Within the control activities the Office also contributed to the coordination of the cooperation with foreign affiliate DPAs. Within the supervision, on request of the affiliate DPA in the Hungarian Republic, the Office verified the status of personal data protection in business companies providing call centre services.
Sanction Activities	
Sanctions	
Penalties	Within the control activities the Office has aimed mostly at prevention resulting in minimal sanctioning of controllers and processors. In the evaluated period of time the Office imposed a total of 5 fines in the total amount of EUR 8 050.
DPOs	
Figures on DPOs	42 411

B. Information on case-law

2012 has ended a long-standing lawsuit between the Office and a business company which as a collector of personal data processed the personal data and also operated activities related to the extrajudicial collection of claims as well as other associated tasks for a processor which as a non-bank subject has provided untied financial loans. This collector has claimed for a judicial review and subsequently for annulment of an administrative decision of the Office that imposed the fine to the collector for unauthorised disclosure of personal data when on the postal envelopes the collector noted the information about the fact that the addressee is evader and thus he unlawfully disclosed the personal data of data subjects about their economic identity. The court found that the examined decision is factually and legally correct and that the Office decided correctly and in accordance with the law.

C. Other important information

Personal data protection as an integral part of the right to privacy of individuals is one of the fundamental rights and freedoms guaranteed by the Constitution of the Slovak Republic. The right to personal data protection is a young but rapidly developing area. Twenty years has passed since the establishment of the Slovak Republic, however, during these years the issue of the protection of personal data has found its application and importance in practice as, due to the development of social relations and expansion of

information technologies, is growing. These influences had significant impact on movement and understanding of the existence of legislation in the area of personal data protection. New challenges and demands have come to the forefront which has influenced the measures of processing and transferring an increasing amount of personal data, as well as the access to them.

Supervision of personal data processed on the territory of Slovak Republic was entrusted to the Office since 1 September 2002 by the Act No 428/2002 Coll. which within its scope of powers monitors the status of protection of personal data. Detection of the status of personal data protection can be seen as a long-term process that is continuously formed during the ensuring of each individual task by the Office, particularly during the provision of public or expert consultation and during the executing of inspection activities by the Office. In the evaluated period of time the question of adequate fulfilment of tasks was the main issue while the Office was facing a lack of financial and staff provision.

There is no doubt that the issue of personal data protection is an easy single topic. This fact results from the past experiences of the Office. The outcomes of the investigation activities of the Office and the huge amount of questions asked by the public about the application of the Act indicates the lack of knowledge and application of the rules of personal data protection in practice, especially for small and medium entrepreneurs and local government authorities which also faced adverse economic development and saving principles.

On the other hand, thanks also to the recent social and technological developments, the statistics related to the performance of the Office show that there is an increased awareness in the existence of a right to personal data protection and an interest in ensuring legal and secure data processing. These particular circumstances involved, irrespective of the Office's activities, in growing and improving caution and prevention on the side of natural persons. Therefore public awareness can be seen as the first step towards the fulfilment of the obligations in the area of personal data protection and towards the application of their rights in everyday life.

Generally speaking, the status of personal data protection in Slovak Republic was satisfactory in the evaluated period of time. However, it is in the interests of all concerned subjects that the level and the quality of personal data protection of natural persons will reach, with further development, such levels of protection as required.

SLOVENIA

A. Summary of activities and news

We could mark the year 2012 as a year of ambitious plans of the State for additional informatisation of large public databases following an expeditious procedure, and the growth of the appetites of the public sector for ever-more expanding processing of personal data. It is alarming that the State, that should have been protecting privacy in accordance with the Slovenian Constitution, is trying to erode the foundations of data protection law.

The Information Commissioner dealt with more than 80 proposals for amendments to legislation, that provide for personal data collection and processing, which is more than a third more than in 2011. Many of the proposals are, in our opinion, an attempt to legalise disproportionate collection and processing of personal data that will neither contribute to administrative procedures being simpler nor to austerity measures, but will on the other hand lower the level of privacy protection of citizens. Among the acts that have been in the process of amendments are the Electronic Communications Act, the Act on Police Tasks and Authorities, the Labour Market Regulation Act, the Inheritance Act, the Public Procurement Act and the Public Administration Act. Most of the proposals for amendments show a complete lack of data protection impact assessments that should have been presented in the context of new planned data processing activities. It seems that the financial crisis has not touched the informatisation area as much as other parts of the public sector. On the contrary, many of the intended informatisations will bring considerable costs.

The Information Commissioner dealt with an extremely high number of cases in the two fields of operation, regarding either requests for an opinion, complaints or appeals. Such circumstances are on the one hand positive, being evidence that individuals are ever better informed and having increased awareness and understanding of the purpose and importance of these two human rights whose implementation and protection fall within the competence of the Information Commissioner. At the same time, such an increase in the number of appeals and cases related to inspections can also be ascribed to certain worrisome actions of liable authorities in the area of access to public information, on the one hand, as well as to the enormous (perhaps too enormous) appetites of various data controllers from the private and public sectors as regards processing personal data.

Regardless of the increasing number of cases, the Information Commissioner strives for an increasing level of responsiveness and professionalism; however, due to the increasing number of cases processed this is barely still attainable. Nevertheless, I am pleased that in 2012 we again succeeded in doing so and that the public recognises our efforts to protect both fundamental rights, i.e. the right to access public information and the right to personal data protection, and thus in the past year it again expressed a high level of trust in the Information Commissioner.

According to research carried out by the Public Opinion and Mass Communication Research Centre, as of January 2013 the level of trust in the Information Commissioner was characteristically high again (52 %), the highest among the examined four supervisory institutions. Since previous measurements also demonstrated a high level of trust and since the percentage has always been in the upper half of the range, a continuous level of trust has clearly been expressed, which makes me extremely satisfied and at the same time compels us to continue with our work and seek ways to improve.

With regard to the area of personal data protection for 2012, the Information Commissioner dealt with 725 inspection cases (6 % more than in 2011) and 158 offence procedures (16 % more than in 2011). In terms of developing trends I would like to draw special attention to cloud computing that is occupying an increasingly important position in terms of data protection and technological development. The potentials of cloud computing are vast, however this should not cause lowering of the level of personal data protection — a fundamental human right. In 2012 the Commissioner published, together with the Cloud Security Alliance (CSA) — Slovenia Chapter, ISACA Slovenia Chapter and Eurocloud Slovenia,

guidelines for data protection in cloud computing, as one of the first authorities in the EU to contribute to the establishment of appropriate standards in this field ([15]). The purpose of the document is to establish common control points, by which users, as well as supervisory authorities, will be able to come to informed decisions regarding the use and oversight of cloud computing services in part where processing of personal data is concerned. The initiatives for safer use and certifications of cloud services, on the other hand, are offered guidelines for future developments with the goal of compliance with personal data protection legislation. The Information Commissioner finds that many cloud service providers do not yet offer to their prospective clients all the information necessary to make an informed choice. Mechanisms still need to be put in place that will allow for differentiation between the providers that are trustworthy and those that are not.

Organisation	Information Commissioner of the Republic of Slovenia
Chair and/or College	Mrs Nataša Pirc Musar
Budget	EUR 1 610 000
Staff	33 employees: the cabinet (2 to 6 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 (10).
General Activity	Data protection and access to public information
Decisions, opinions, recommendations,	143 comprehensive and 2 048 short opinions and recommendations based on requests from data subjects or data controllers.
Notifications	153 notifications on personal data filing systems.
Prior checks	23 prior checks: 7 on biometrics, 5 on transfers of data to third countries, 12 on connection of filing systems.
Requests from data subjects	2 048 requests for opinions/clarifications from data subjects.
Complaints from data subjects	747 complaints from data subjects altogether, 497 complaints qualified. Areas: 226 unlawful transfer or disclosure of data, 144 unlawful collection of data, 118 direct marketing, 72 video surveillance, 44 data security, 153 other. Additionally 63 complaints regarding data subjects' rights were handled.
Advice requested by parliament or government	The legislator and competent authorities drafting the legislation consulted the Commissioner regarding 80 acts and other legal texts, among other the Electronic Communications Act, the Act on Police Tasks and Authorities, the Labour Market Regulation Act, the Inheritance Act, the Public Procurement Act and the Public Administration Act, etc.

([15]) https://www.ip-rs.si/index.php?id=308

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	725 inspections: 245 in public sector, 480 in private sector.
Sanction activities	
Sanctions	158 offence procedures initiated (29 in public sector, 78 in private sector, 51 private persons), of these 17 warnings, 61 admonitions, 58 fines and 7 payment orders issued.
Penalties	The DPA imposed EUR 50 037 of penalties, administrative taxes excluded.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Data on employees' printing

The Information Commissioner received a complaint that the management of a State authority requested a list of all employees and their use of work printers (names, surnames, the number of prints, titles of documents). In the inspection procedure it has been established that the authority needed to monitor the costs of printing and therefore used an application to establish that the employees were actually making irrational and non-ecological use of printing facilities, and also printing personal items. The Commissioner concluded that the authority should not have been collecting the data on the title of the document or the printed website, as these are personal data that are not necessary to effectively manage the processes and cost of printing that needs to be done by the authority. The Commissioner ordered that the said data must not be collected further and that the application be adapted, however, the authority decided not to use the application anymore.

Collection of data for direct marketing online

The Information Commissioner received a number of complaints regarding a data controller performing direct marketing via e-mail, allegedly without the individual's consent to processing of their personal data. In the inspection procedure it has been established that the data controller held in its databases data on more than 100 000 individuals, registered users of its website and users of certain Facebook

applications. The Commissioner concluded that the data controller presented sufficient evidence that it obtained consent from the registered users of its website, however did not present sufficient evidence with regard to Facebook application users, who have allegedly consented by installing different applications. When a user installs a Facebook application the controller's servers should have by default recorded some background data such as the time of installation or IP address or similar. Since the controller did not present any evidence but instead claimed that the sole existence of the data in its data bases testified that the users have consented, the Commissioner ordered for the data to be deleted. The data controller implemented the order.

Biometric measures in a fitness studio

The Information Commissioner received a complaint that a fitness studio performs biometric control over its customers who wish to enter the premises, and has video surveillance cameras installed in locker rooms. In the inspection procedure it has been established that the fitness studio actually performed biometric checking of the customers entering the premises, however the customers were able to choose between a key card with a chip and no biometric data, and biometric checking, which included a template of the customers fingerprint. The controller did not store the customers' fingerprints but only the templates and believed that such activity does not fall under the regime of biometric data processing. The Commissioner clarified that such storing of templates constitutes processing of biometric data. It ordered the fitness studio to stop processing biometric data because it did not have a legal basis for such processing. The PDPA-1 only allows, under certain conditions, implementation of biometric measures over the employees and not customers. It has also been established that the fitness studio performs video surveillance in locker rooms, where this is forbidden by law. The Commissioner ordered the studio to either stop video surveillance of the locker rooms or ensure that the customers have other rooms available where they can change clothes without being monitored.

The visitors of a gambling website redirected to another web address

The Commissioner initiated a procedure against the Office for Gaming Supervision which registered a domain to which all visitors of gaming sites that operate without the government's concession were redirected. In the inspection procedure it has been established that the data controller does not have a legal basis in the law to collect and process the information on the visitors of the gaming sites that operate without the government's concession. The Gaming Act ([16]) provides that access to such websites may be limited but does not provide for any processing of the data of the visitors in such a way that visitors are redirected to the controller's website and their data (such as IP address, time of visit, browser details, etc.) are processed by the controller in such a way. The Information Commissioner held that IP addresses are personal data as well as the data on browser details which provide for a unique fingerprint of the visitor. The Commissioner ordered the controller to delete from its data bases the data that could uniquely identify the visitors and not to collect those data in the future. The Controller executed the order and filed an appeal to the Administrative Court against the Commissioner's decision. The Court has not decided yet on the merits of the case.

Processing of personal data in bicycle renting service, BicikeLJ

The Information Commissioner received a number of complaints regarding a new bicycle renting service, BicikeLJ, where the data controller requested a number of personal details of the users who wished to register for the service, including such that were not necessary in relation to the service. In the inspection procedure it has been established that the data controller collects and processes different personal data based on the type of service a user wishes and on the type of payment (credit card or direct debit). The legal basis is the contract between the user and the service provider. It has been established that in

([16]) Official Gazette RS, No 27/1995 47/2006, s spremembami, v nadaljevanju ZEN.8427/15527with amendments.

none of the cases the data controller can show that it requires for the fulfilment of the contract the data on the gender, and mobile phone number of the users. Additionally, for the users that pay for the service with a credit card the data controller should not require the home address of the users. The Commissioner established that the said data may be collected and processed based on user consent, however such consent must be freely given and the user must be presented with a choice whether it wishes to supply the data to the service provider, as those data are not necessary for the fulfilment of the bike renting contract. The data controller executed the order and filed an appeal to the Administrative Court against the Commissioner's decision.

C. Other important information

Information Commissioner employees regularly participate in international seminars and conferences where they often present their own papers.

As the national supervisory authority for the protection of personal data, the Information Commissioner cooperates with the competent bodies of the European Union (EU) and the Council of Europe engaged in personal data protection.

In 2012, the Information Commissioner actively participated in six EU working bodies engaged in supervision of the implementation of personal data protection within individual areas of the EU, namely the following:

- the Article 29 Working Party for personal data protection, as well as in four of its subgroups (the Technology Subgroup, the Future of Privacy Subgroup, the Binding Corporate Rules (BCR) Subgroup, and the Borders, Travel and Law Enforcement (BTLE) Subgroup);
- the Europol Joint Supervisory Body;
- the Joint Supervisory Authority for Schengen;
- the Joint Supervisory Authority for Customs;
- at co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of CIS;
- at co-ordination meetings of the European Data Protection Supervisor (EDPS) together with state national authorities for the protection of personal data (EURODAC).

In 2012, the Head of the Information Commissioner continued to hold the position of Vice-Chairman of the Europol Joint Supervisory Body. In February 2012 a Deputy Information Commissioner participated in the international inspection group that carried out an inspection regarding personal data protection at Eurojust's headquarters in the Hague. The Information Commissioner also regularly participated in the International Working Group on Data Protection in Telecommunications (IWGDPT). Once again in 2012, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

In 2012, the Information Commissioner hosted representatives of similar institutions from a number of countries, such as Serbia, Georgia, Macedonia and Albania to whom it presented its activities and good practices in its fields of competence. As a Junior Partner it successfully finished the Twinning project IPA 2009, No MN/09/IB/JH/03 — Implementation of Personal Data Protection Strategy in Montenegro — and it started the implementation of the Twinning Light Project SR/2009/IB/JH/01 — Improvement of Personal Data Protection — which is focused on improving personal data protection in Serbia.

In 2012, the Information Commissioner continued and in September finished its work within the European LAPSI project (Legal Aspects of Public Sector Information), which is intended to establish a

thematic network of experts in the field of the reuse of public information in order to remove obstacles to its implementation that occur in practice.

SPAIN

A. Summary of activities and news:

Even more so than in previous years, 2012 was marked by a remarkable growth of the activity of the Agency, notably in data processing notification and inspection activities areas, with positive growth percentages of 15 % and 40 % respectively. Throughout 2012 we have been working on measures to simplify and facilitate exercise of the rights of citizens as well as to ease regulatory compliance. In that sense, particular reference is owed to the setting up of our e-services platform - https://sedeagpd.gob.es/sede-electronica-web/ — as well as the enhancement of all the information services provided through our website.

With regard to inspection activities and the exercise of sanctioning powers, it is relevant to point out that, even though the figures on punitive resolutions remain stable, there is a substantial increase on the resolutions issuing written warnings, actually a 34.2 % with regard to 2011. The use of this possibility, jointly with the set of criteria that can now be used to graduate the amount of the penalties, allows a substantial gain on tempering the severity of the sanction to the gravity and real consequences of the infringement.

The Agency is also maintaining its effort on ensuring a better protection for children. In that regard, we have been intensively working along the year on an educational website aiming to offer relevant information and tools for both children and educators that is likely to be launched in the last quarter of 2013.

Another area of intense activity has been the implementation of the reform of the E-privacy Directive that was transposed into national law by a Royal Decree dated April 2012. Since that moment, the Agency has been working with all the implied stakeholders at national and international levels. As a result of the efforts, documents on guidance and tools related to the right implementation of cookies using provisions and data breach notifications are to be issued in 2013.

Organisation	Spanish Data Protection Agency
Chair and/or College	José Luis Rodríguez Álvarez
Budget	EUR 13 929 550
Staff	159
General Activity	
Decisions, opinions, recommendations	11 907
Notifications	630 251
Prior checks	n/a
Requests from data subjects	111 933
Complaints from data subjects	10.787

Advice requested by parliament or government	292
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	2266
Sanction Activities	
Sanctions	896
Penalties	EUR 21 054 656.02
DPOs	
Figures on DPOs	n/a

B. Information on case-law

A first reference has to be done to the Supreme Court's decision dated February 2012 settling appeals related to the Royal Decree 1720/2007, of 21 December, which approves the regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data. The decision declared Article 10.2.(b) of the regulation not valid, working on a preliminary ruling of the ECJ (Judgment of 24.11.2011 in Cases C-468/10 and C-469/10 —ASNEF and FECEMD).

Other relevant decisions from the Supreme Court are the following:

Information related to the conviction for an offence of sexual abuse cannot be considered data related to sex life in the sense of Article 8 of the Directive 95/46;

A consent clause allowing the sending of commercial offers from a group of companies might be deemed sufficient to send job offers from the same entities;

The burden of proof related to the compliance with the duty of information rests on the controller;

Video-surveillance devices can only be used to monitor compliance with the working time rules if the individual has been duly informed in advance of that possibility;

There is a breach of the duty of secrecy when health data — in this case, the list of patients receiving treatment with methadone — is published on the notice board of a health centre. In the same line, when data is made accessible through a peer to peer file sharing system;

Also in relation with the duty of secrecy, the publication in an official journal of the conviction for a criminal offence affecting a public employee is considered a breach of the duty of secrecy;

The mere existence of a complaint does not oblige the supervisory authority to start an infringement procedure.

The National High Court (Audiencia Nacional) has been also quite active in 2012 dealing with data protection issues. There are also some relevant decisions as follows:

- Images of children can only be uploaded and shown on social networks websites with the previous consent of parents or legal guardians. In the same line, it is mandatory to put in place

mechanisms favouring age verification and to get parental consent when a controller aims to process children's data in the scope of marketing campaigns on the Internet.

- As regards to the Supreme Court's decision on the application of the legitimate interest as legal basis for data processing, there are several decisions of the National High Court applying the ruling, notably the following:
    - The legitimate interest of a newspaper was considered more prevalent when publishing details of sanction notices related to individuals holding a public office. In the same way, the publishing of identification details of the applicants to positions related to public employment;
    - The legitimate interest of a trade union was also considered more prevalent for the processing of staff data in-house and for purposes directly linked to worker representation tasks;
    - In the same line, the use of contact data from the members of a professional chamber by other members in the course of an internal electoral process;
    - On the other hand, it was not considered more prevalent the interest for compiling a database with data of thirty-seven million people when the alleged interest was the mere intention of marketing the database.
- It was considered lawful adding images as evidence obtained by a private investigator to a court case file when those images were accepted by the judge in the course of the proceeding. On the contrary, it was considered unlawful to include images of an individual as part of the show window of a photographer without the consent of the individual.
- It was considered health data processing when printing on a postal envelope the sentence 'celiac patient' when advertising products. Also related to sensitive data, it was considered sex-life data processing to create a false profile pretending to be a third person in a social network mainly addressed at the homosexual community.

C. Other important information

The so-called Google case has been also playing an important role along the year because of the relevant questions at stake as well as the involvement of the European Court of Justice at the request of the Spanish National High Court. The case as such started with the request made by a citizen to exercise the right of opposition with regard to the processing made by a newspaper — a public notice published several years ago — related to information that he considered not only outdated but irrelevant despite the fact that it could affect him in his present life since it can be easily found on the Internet through a search engine.

The newspaper denied the deletion of the data by arguing it was published due to a legal obligation resulting from an order coming from a competent authority.

In a second step, the citizen exercised his right to object before Google, requesting the deletion of the links pointing to the piece of news in the newspaper's website. The addressed entity was Google Spain, SL. The request was also rejected by the entity.

Finally, the citizen lodged a complaint before the Spanish DPA with the aim to ensure that his rights were duly exercised. He addressed both entities, Google Inc. and Google Spain, SL.

In response to the claim the Spanish DPA issued a decision requesting both Google Inc. and Google Spain to attend the requirement. No action was taken with regard to the newspaper.

Both entities went then to the National High Court against that decision. The case was taken into consideration by the Court jointly with several previous decisions on similar issues. Due to the increasing

amount of requests and the nature of the issues under discussion, the Court decided to carry out a public hearing with both parties presenting their views. The Court decided also to address the EU Court of Justice for a preliminary ruling.

There are two main issues at stake:

a) On one hand, the applicability of Directive 95/46 to the services offered by Google Inc. to EU citizens. In that aim, the Court tabled a battery of questions related to the applicability of Article 4.1 of the Directive, since Google Spain, SL, a subsidiary of Google Inc., is doing business with the search engine and also considering that Google Spain, SL has been expressly appointed by Google Inc. as its representative in order to transfer to the latter claims and legal requests coming from Spanish citizens. The Court also asked for clarification on the notion of 'equipment situated on the territory of a Member State'. In that sense the Court made a direct mention of Article 8 of the ECHR, stating that it would be fair to apply the law of the country where the conflict takes place in order to ensure effective protection for the citizens.

b) b. On the other hand, a set of questions were made with regard to the very nature of the search engines. First, and taking into account the definition of data processing stated by the Directive, the Court asked about the possibility of considering the indexing processing personal data processing in the sense of Directive 95/46. Provided that the answers were yes, the second question would inquire about the real nature of the legal responsibilities of the entity offering the service... direct, full or simply subsidiary of the data controller responsible for the web where the information was originally processed. Given that, and according to the ECJ criteria, it would be made possible to make an interpretation in the sense of directly addressing the controller of the search engine in order to avoid indexing the affected information.

A final decision is expected for the last quarter of 2013.

SWEDEN

A. Summary of activities and news:

Supervision

Supervision in 2012 was directed towards personal data processing in relation to e-government, health and medical data, research, social welfare, law enforcement, confidential information about students in schools, competence data bases, political parties' data about members and smart phone apps in the bank sector, etc.

Awareness raising

Media articles regarding our activity reached a new high in 2012. There was also a significant increase in questions from the public, by phone and e-mail as well as in visits on our website. Similar to previous years, we published a leaflet containing the most important privacy issues during the year, the Privacy Year 2012.

Organisation	Data Inspection Board
Chair and/or College	Director General Mr Göran Gräslund (As of 1 June 2013, the Director General is Mrs Kristina Svahn Starrsjö)
Budget	SEK 36 931 000 SEK = EUR 3 987 841
Staff	Approx. 45
General Activity	
Decisions, opinions, recommendations	115 opinions on legislative proposals on request from the Government offices 68 opinions in consultation with data protection officials 6 guidelines, recommendation and reports
Notifications	
Prior checks	247 (mostly regarding research and processing of DNA data)
Requests from data subjects	Our helpdesk: 8 000 phone calls, 5 600 e-mails Formal requests: 219
Complaints from data subjects	323
Advice requested by parliament or government	See the decisions, opinions etc above
Other relevant general activity information	Press releases: 69, Lectures and seminars: 52

Inspection Activities	
Inspections, investigations	267 (finalised inspections) (43 field, 143 desk and 81 questionnaire inspections) Key topics: police, camera surveillance, Internet publication, bank apps, competence databases, secret data in schools, political parties and their members
Sanction Activities	
Sanctions	---
Penalties	Not applicable
DPOs	
Figures on DPOs	6 825

B. Information on case-law

In a decision from March 2012, the Supreme Administrative Court turned down an appeal from two upper secondary schools which had installed indoor camera surveillance. The Data Inspection Board had ordered the schools to stop the surveillance during daytime. The Board stated that camera surveillance can only be permitted if there is a substantial need for such surveillance that outweighs the students' right not to be monitored. The schools appealed to the Administrative Court of Appeal who rejected the appeal. The Supreme Administrative Court confirmed this decision and said that camera surveillance in classrooms, hallways, the school library and recreation rooms etc. must generally be seen as an infringement of the data subjects' privacy. The Data Inspection Board has since then produced a check list in order to facilitate for schools to assess whether camera surveillance is permitted or not according to the Personal Data Act.

In another case, the Supreme Administrative Court confirmed the Data Inspection Board's decision in which the Board had ordered the social insurance office to perform a risk and vulnerability assessment regarding their text messaging service for reporting sick leave in order to obtain social benefits. The Supreme Administrative Court's decision confirmed the Data Inspection Board's view that it was the insurance office who decided the purpose and means of the processing and that they therefore were responsible for the personal data processing that the text messaging service involved.

UNITED KINGDOM

A. Summary of activities and news:

Organisation	The UK Information Commissioner's Office
Chair and/or College	Information Commissioner Christopher Graham
Budget	GBP 20 million per annum
Staff	330 FTEs
General Activity	
Decisions, opinions, recommendations	Educating and Guiding The ICO published a code of practice on managing the data protection risks related to anonymisation; the first European data protection authority to publish a code on the issue. The ICO also published new guidance on cloud computing, deleting personal data and asset destruction. We also consulted with the public on a new Subject Access Code of Practice. Media Activity The ICO took 1 673 calls from journalists and carried out 113 media interviews. We also issued 50 news releases that generated extensive and generally positive press coverage. 900 updates and additions were made to the ICO's website and 45 pieces of guidance were published or substantially updated.
Notifications	372 369
Prior checks	N/A
Requests from data subjects	213 813 answered calls on the ICO's helpline 29 042 written advice queries answered
Complaints from data subjects	20 515 (total relating to the Data Protection Act 1998 and Privacy and Electronic Communications Regulations 2003/11)
Advice requested by parliament or government	The ICO constantly engages with the government advising on data protection-related legislation through giving evidence to Parliament and responding to consultations. A summary of activity this year is below: Parliamentary evidence

	Justice Select Committee — Opinion on the European Union Data Protection Framework Proposals Scottish Affairs Committee - Inquiry into Blacklisting in Employment. Consultation responses Cabinet Office — Introducing a statutory register of lobbyists Citizens Advice — Consultation on Consumer Future Consumer Focus — Proposals for a regulated industries unit Department for Communities & Local Government — Social housing fraud Department for Education — Proposed amendments to Individual Pupil Information Prescribed Persons Regulations Department for the Environment & Climate Change — Smart data access and privacy Department of Health — Consultation on strengthening the NHS Constitution Department of Justice (NI) — Making a difference: Improving access to justice for victims and witnesses of crime: a five year strategy Director of Public Prosecution — the DPP's interim guidelines for prosecutors on assessing the public interest in cases affecting the media HM Revenue & Customs — Implementing the UK-US FATCA Agreement Home Office — Protection of Freedoms Act 2012 — Surveillance Camera Code of Practice consultation Law Commission — Contempt of court consultation Law Society — Reforming the law of taxi and private hire services Ministry of Justice — Getting it right for victims and witnesses Ministry of Justice — Transforming Rehabilitation — a revolution in the way we manage offenders Ministry of Justice — Swift & Sure Justice: The Government's plans for reform of the criminal justice system Nominet — Consultation on a new .uk domain name service Office of National Statistics — Future dissemination strategy for the publication of national statistics on crime in England and Wales The Leveson Inquiry — response to the report on the culture, practices and ethics of the press Welsh Government — Registering and monitoring home-based education Welsh Government — The Draft Human Transplantation (Wales) Bill and Explanatory Memorandum

	Welsh Government — Providing support for council tax in Wales
Other relevant general activity information	ICO annual Data Protection Officer Conference The Information Commissioner welcomed several hundred data protection officers from all over the UK to Manchester for the fifth annual Data Protection Officer Conference. David Smith, Deputy Commissioner and Director of Data Protection gave a keynote speech updating participants on the latest EU developments to update the current law. EU developments The ICO published its Initial Analysis on the EU data protection reform in February 2012. The ICO held a stakeholder meeting in Spring 2012 and worked with other UK policy stakeholders and the Ministry of Justice to examine the implications of and to raise awareness about the new EU proposals. Enforcement The value of the penalties imposed by the ICO under the Data Protection Act and the Privacy and Electronic Communications Regulations in the last year stands at just over GBP 2.6 million (before early payment reductions). With one exception: the penalties issued under the Data Protection Act were for failing to keep personal information secure. The area of ICO enforcement work that grabbed the most headlines was our action to tackle cold calls and spam text messages. In March we set up an online reporting tool so that people can tell us about the messages they are receiving. More than 155 000 people have now used this tool to provide us with information, which we then use to inform our investigations. Audit and Good Practice The ICO has introduced outcomes reports which summarise common audit themes; highlighting both good practice and areas for improvement in the private, health, local government, central government, police and probation sectors. We have disseminated good practice by giving presentations on audits and their outcomes at selected forums. We also developed and ran a central advisory visit workshop which allowed us to reach even more organisations. The ICO asked over 400 schools to complete a data protection questionnaire. We then used the results to produce a report indicating good practice and areas for improvement, and giving practical advice on the application of the Data Protection Act.

	Ensuring effective outreach to all regions In February the ICO held a series of highly successful hands-on workshops across Wales, highlighting basic good practice in personal data handling. We targeted public and third sector staff on the front line of service delivery, with possibly less experience of data protection, drawing heavily on examples of good and bad practice uncovered by the ICO's audit and enforcement departments. Data protection in the health sector The ICO participated in the Department of Health Information Governance Review Panel. The ICO hopes that this work will help transform information governance in an area where some of our most sensitive personal details are held. Anonymisation The ICO set up and funded the UK Anonymisation Network Launched alongside the ICO's new Code of Practice on Anonymisation. The aim of the network is to enable the sharing of anonymisation good practice and find solutions to challenges, making use of a website, social media and events, and case studies. Following a tender process the funding to run the network was awarded to a consortium of the University of Manchester, University of Southampton, Office for National Statistics and the Open Data Institute. Leveson Inquiry — privacy and the press Privacy intrusion by the press is currently an important topic on the UK Government and independent regulators' agenda. The Information Commissioner's Office made a preliminary statement ahead of its official response to the Leveson Report following the Leveson Inquiry (led by High Court judge Lord Justice Leveson) on the Culture, Practices and Ethics of the Press in the UK. We participated in the Inquiry giving an account of our previous work uncovering the media's role in the illegal trade in personal information. Our future work will be against the backdrop of the government's plans for future regulation of the media.
Inspection Activities	
Inspections, investigations	58 audits and 35 audit follow-ups. 78 advisory visits
Sanction Activities	
Sanctions	23

Penalties	17 undertakings, 2 enforcement notices, 6 prosecutions
DPOs	
Figures on DPOs	The Data Protection Act 1998 requires every data controller (e.g. organisation, sole trader) who is processing personal information to register with the ICO, unless they are exempt. More than 370 000 organisations are currently registered.

B. Information on case-law

—

C. Other important information

The UK Protection of Freedoms Act 2012 contains the following provisions that relate to the ICO's activities:

Part 1; regulation of biometric data. This includes provisions relating to the destruction, retention and use of fingerprints, footwear impressions and DNA samples and profiles. It also includes provisions about the protection of biometric information of children in schools.

Part 2; regulation of CCTV and other surveillance camera technology. This will lead to the introduction of a new Surveillance Camera Commissioner.

Part 3; provides protection of property from disproportionate enforcement action. These regulations relate to powers of entry, parking enforcement powers and potential increased use of ANPR (automatic number plate recognition) technology.

Part 5; safeguarding vulnerable groups and criminal records. It also introduces the Disclosure and Barring Service (which replaces and combines the responsibilities of, the Criminal Records Bureau and the Independent Safeguarding Authority). This part also provides that certain sex offences are disregarded.

Part 6; changes to the Data Protection Act 1998. The changes relate to:

- The appointment and tenure of the Information Commissioner from a five- to seven-year term;
- The alteration of the role of theSecretary of State in relation to guidance powers;
- The removal of Secretary of State consent for fee-charging powers;
- The removal of Secretary of State approval for staff numbers and terms.

Chapter Three

European Union and Community Activities

3.1. EUROPEAN COMMISSION

3.1.1. **Commission proposal for a regulation of the European Parliament and of the Council** COM(2012) 11 of 25 January 2012 on the protection of individuals with regards to the processing of personal data and on the free movement of such data **(General Data Protection Regulation).**

3.1.2. **Commission proposal for a Directive of the European Parliament and of the Council** COM(2012) 10 of 25 January 2012 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and **the free movement of such data.**

3.1.3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2012) 09 Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century.

3.1.4. **Commission Staff Working Document** SEC(2012) 75 of 25 January 2012 Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around EUR 2.3 billion a year. The initiative will help to reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe. The Commission's proposals update and modernise the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights in the future. The policy Communication sets out the Commission's objectives, and two legislative proposals — a **Regulation** setting out a general EU framework for data protection and a **Directive** on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

Key aims of the reform include a **single set of rules** on data protection, valid across the EU. Unnecessary **administrative requirements,** such as notification requirements for companies, will be removed. This should save businesses around EUR 2.3 billion a year. Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors — a requirement that has led to unnecessary paperwork and costs businesses an estimated EUR 130 million per year, the Regulation provides for increased **responsibility and accountability** for those processing personal data.

Companies and organisations will have to notify the national supervisory authority of serious **data breaches** as soon as possible (if feasible within 24 hours). Organisations will only have to deal with a **single national data protection authority** in the EU country where they have their main establishment. Likewise, people can refer to the **data protection authority** in their country, even when their data is processed by a company based outside the EU.

Wherever **consent** is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed. People should have easier **access to their own data** and be able to **transfer personal data** from one service provider to another more easily (right to data portability). This will improve competition among services. A **'right to be forgotten'** will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it. EU rules will apply if personal data is **handled abroad** by companies that are active in the EU market and offer their services to EU citizens.

Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules, leading to penalties of up to EUR 1 million or up to 2 % of the global annual turnover of a company.

The new **Directive** will apply general data protection principles and rules for **police and judicial cooperation** in criminal matters. The rules will apply to both domestic and cross-border transfers of data.

3.1.5. **Conference** of 19 March 2012 on Privacy and the Protection of Personal Data, Washington, DC/Brussels.

This Conference, held simultaneously in Washington and Brussels, provided a forum for US and EU stakeholders from public and private sectors to obtain comprehensive, accurate and up-to-date information on EU data protection principles and the ongoing reform, and to discuss US and EU perspectives focusing on commercial privacy.

3.1.6. **Agreement** of 1 June 2012 between **the European Union and Australia** on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service — L 186, 14/07/2012, p. 4.

The Agreement provides that the purposes for which data may be sent to the Australian Customs and Border Protection Service are the prevention, detection, investigation and prosecution of terrorist offences and serious transnational crime. The agreement contains definitions of those crimes for a better understanding of its scope. PNR data that the Australian authorities may use are listed in an annex to the agreement.

The Australian Customs and Border Protection Service may only access EU PNR data on the basis of transfers of such data by carriers via a 'push' system.

Protection of personal data and the right of individuals to seek access to and correction of their personal data apply irrespective of nationality or place of residence.

Periodical review of the implementation of the agreement, including its operational effectiveness, will take place four years after its entry into force.

Sensitive data (such as personal data that may indicate racial or ethnic origin, political opinions, religious beliefs or trade union membership or concern health or sex life) shall be filtered out and deleted by the Australian Customs and Border Protection Service; however, PNR normally does not contain sensitive data.

The Agreement provides for a data retention period of five and a half years, and after three years, the data will be masked.

The Australian Customs and Border Protection Service will aim to ensure the sharing of analytical information derived from EU PNR data with the competent authorities of EU States and, in appropriate cases, with Europol and Eurojust, to strengthen the police and the judicial cooperation between Australia and the EU and to enhance reciprocity.

The agreement has a term of seven years to ensure legal certainty for a considerable period, and may be renewed for a subsequent period of seven years.

It includes standards on monitoring correct implementation, review and effective dispute resolution, as well as the modalities of transfer of PNR data aim to provide legal certainty to air carriers and keep costs at an acceptable level. PNR data should be transferred by using the 'push' system and the number of times that data is transferred before each flight is limited to a maximum of five per flight.

3.1.7. **Agreement** of 1 July 2012 between **the European Union and the United States of America** on the processing and transfer of **Passenger Name Record** (PNR) data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection — L 215, 11 August 2012, p. 5.

According to this Agreement, the purposes for which the PNR data may be sent to the US Department of Homeland Security are the prevention, detection, investigation and prosecution of terrorist offenses and related crimes and other transnational crimes punishable by a sentence of imprisonment of three years or

more. The agreement contains definitions of those crimes for a better understanding of its scope. PNR data that the US authorities may use are listed in an annex to the agreement.

Air carriers transfer PNR data to the Department of Homeland Security using the 'push' method.

All passengers, irrespective of nationality and country of residence, have access to redress mechanisms in relation to DHS administrative decisions. Implementation of the Agreement is reviewed periodically. In addition, the agreement shall be evaluated jointly four years after its entry into force.

Sensitive data (such as personal data that may indicate racial or ethnic origin, political opinions, religious believes or trade union membership or concern health or sex life) shall be filtered and masked out and such data shall not be further processed or used, unless in exceptional circumstances where the life of an individual could be imperilled or seriously imperilled. However PNR data normally do not contain sensitive data.

Data may be retained for five years in an active database and up to 10 years in a dormant database. During this period the data are gradually depersonalised and masked and access to it is further restricted.

The Department of Homeland Security aims to ensure the sharing of analytical information derived from EU PNR data with the competent authorities of the EU states, and in appropriate cases with Europol and Eurojust, to strengthen the police and judicial cooperation between the US and the EU, and to enhance reciprocity.

The Agreement has a term of seven years to ensure legal certainty for a considerable period, and may be renewed for a subsequent period of seven years.

3.1.8. **Commission Implementing Decision** of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704) Text with EEA relevance — OJ L 227, 23 September 2012.

For the purposes of Article 25(2) of Directive 95/46/EC, the Eastern Republic of Uruguay is considered as ensuring an adequate level of protection for personal data transferred from the European Union.

3.1.9. **Commission Staff Working Document** SWD (2012) 454 of 14 December 2012 Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Programme of October 2012

The second joint review was conducted jointly by a US review team and an EU team. According to Article 13(3), the Commission represents the EU in the joint reviews. The EU review team was therefore headed by a senior Commission official and consisted of three members of Commission staff and three external experts, namely two data protection experts, and an expert with judicial experience, who supported the Commission in reviewing the agreement.

The review was carried out in two main steps: on 4 October 2012 in The Hague, at Europol premises, and on 30 and 31 October 2012 in Washington, at the US Treasury Department (hereinafter 'the Treasury').

Both review teams first met in The Hague, at Europol headquarters, and were informed by Europol senior staff and experts on Europol's implementation and practical application of the Agreement. The teams visited the secure location where Europol handles the US requests and met the persons having access to the data in question.

To prepare the visit in Washington, the EU team had sent an advance questionnaire to the Treasury, with specific questions on all the aspects of the review as specified in the Agreement. The Treasury provided written replies to the questionnaire. The EU review team also put further questions to Treasury officials and in order to address all the parameters of the Agreement.

The review teams were granted access to relevant Treasury premises, including the site where the TFTP is operated. For security reasons, review team members were required to provide advance evidence of their security clearances to access the TFTP facility. The review teams were given a live demonstration of searches performed on the provided data, with the results shown and explained on screen by the analysts, while respecting the applicable US confidentiality requirements.

The review teams had direct exchanges with Treasury personnel responsible for the TFTP programme, the overseers who review the searches of the data provided under the TFTP Agreement, and the full-time auditor of the TFTP employed by the Designated Provider. The review teams did not carry out any system checks or controls on the basis of log files.

The EU review team is satisfied that the recommendations presented in the report of March 2011 on the first Joint Review have been followed up to a large extent, thus improving the implementation of the Agreement. Providing more verifiable insights into the actual added value of the TFTP, preferably by public information without endangering the effectiveness of this instrument and respecting the need for confidentiality of the methods and procedures used, remains a challenge.

The EU review team noted further improvements of the verification and oversight mechanisms in particular, some of which go beyond what is required in the Agreement. Overall, the implementation of the agreement more than two years after its entry into force has attained a satisfactory level of implementation, with also the EU increasingly profiting from it under the specific reciprocity arrangements.

3.1.10. Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) Text with EEA relevance — OJ L 28/12, 30 January 2013.

For the purposes of Article 25(2) of Directive 95/46/EC, New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the European Union.

3.2. EUROPEAN COURT OF JUSTICE

3.2.1. Judgment of the Court (Third Chamber) of 22 November 2012 — Josef Probst v mr.nexnet GmbH **(Case C-119/12):** By its question the referring court asked whether, and in what circumstances, Article 6(2) and (5) of Directive 2002/58 allowed a service provider to pass traffic data to the assignee of its claims for payment, and allowed the latter to process those data.

According to Article 6(2) of Directive 2002/58, traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed since it authorises processing of traffic data not only for the purpose of billing, but also for that of debt collection. By authorising traffic data processing 'up to the end of the period during which the bill may lawfully be challenged or payment pursued', that provision relates not only to data processing at the time of billing, but also to the processing necessary for securing payment thereof.

According to Article 6(5) of Directive 2002/58, traffic data processing authorised by Article 6(2) 'must be restricted to persons acting under the authority of [service] providers of the public communications networks and publicly available electronic communications services handling billing' and 'must be restricted to what is necessary' for the purposes of such an activity.

It follows that a service provider is authorised to pass traffic data to the assignee of its claims for payment for the purpose of their recovery, and that the assignee is authorised to process those data on condition, first, that it acts 'under the authority' of the service provider as regards the processing of those data and, second, that it processes only traffic data which are necessary for the purpose of the recovery of those claims.

In the absence of clarification as to the exact scope of the concept of 'under the authority', its meaning must be determined by considering its usual meaning in everyday language, while also taking into account the context in which it occurs, and the purposes of the rules of which it is a part. In everyday language, a person acts under the authority of another where the former acts on instructions and under the control of the latter.

Article 5(1) of Directive 2002/58 provides that Member States are required to ensure the confidentiality of communications by means of a public communications network and publicly available electronic communications services and the related traffic data. Article 6(2) and (5) of Directive 2002/58 contain an exception to the confidentiality of communications laid down in Article 5(1) by authorising traffic data processing in accordance with the requirements of billing services. As it constitutes an exception, that provision, including the words 'under the authority', are to be interpreted strictly. Such an interpretation requires that the service provider has an actual power of supervision which enables it to determine whether the assignee of the claims for payment is acting in compliance with the conditions imposed on it.

Article 6(5) of Directive 2002/58 must therefore be interpreted in the light of the equivalent provisions in Directive 95/46, Articles 16 and 17 of which set out the level of control that the controller must exercise over the processor which it appoints, that that processor acts only on the controller's instructions and that the controller ensures compliance with the measures agreed in order to protect personal data against any form of unlawful processing. Even if Article 6(5) of Directive 2002/58 authorises the processing of traffic data by third persons for the purpose of collecting debts, thereby enabling it to concentrate on the supply of electronic communications services, that provision seeks to ensure, by providing that the processing of traffic data must be restricted to persons acting 'under the control' of the service supplier, that such externalisation does not affect the level of protection of personal data enjoyed by the user.

It follows that the assignee acts only on instructions and under the control of the service provider, and the contract between the service provider and the party to which claims are assigned must ensure the lawful processing of traffic data by the latter, and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee. It is for the national court to determine whether those conditions are met.

The court ruled that Article 6(2) and (5) of Directive 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 (Directive on privacy and electronic communications) must be interpreted as authorising a provider of public communications networks and of publicly accessible electronic communications services to pass traffic data to the assignee of its claims for payment in respect of the supply of telecommunications services for the purpose of recovery of those claims, and as authorising that assignee to process those data on condition, first, that the latter acts under the authority of the service provider as regards the processing of those data and, second, that that assignee confines itself to processing the traffic data necessary for the purposes of recovering the claims assigned. Irrespective of the classification of the contract of assignment, the assignee is deemed to act under the authority of the service provider, within the meaning of Article 6(5) of Directive 2002/58, where, for the processing of traffic data, it acts exclusively on the instructions and under the control of that provider. In particular, the contract concluded between them must contain provisions capable of guaranteeing the lawful processing, by the assignee, of the traffic data and of enabling the service provider to ensure, at all times, that that assignee is complying with those provisions.

3.2.2. Judgment of the Court (Grand Chamber) of 16 October 2012 — European Commission v Austria **(Case C-614/10):** The Commission instituted proceedings against Austria for incorrectly transposing the second subparagraph of Article 28(1) of Directive 95/46 in that Austrian national legislation does not allow the Austrian data protection authority, the Datenschutzkommission (DSK) to exercise its functions 'with complete independence'. The Commission claimed that, because the managing member of the DSK had to always be an official of the Federal Chancellery, all the day-to-day business of the DSK was thus *de facto* managed by a federal official, who remained bound by the instructions issued by, and subject to supervision by, the Federal Government. The Commission further claimed that by being structurally integrated with the other Federal Government departments, the DSK was not independent in either organic or substantive terms. All DSK staff members were under the authority of the Federal Chancellery and were thus subject to its supervision. Finally, the Commission relied on a provision of Austrian law providing for the Federal Chancellor's right to be informed.

The Court noted that Article 28(1) of Directive 95/46 required Member States to set up one or more supervisory authorities, having complete independence in exercising their functions, for the protection of personal data, and that this requirement also derives from the primary law of the European Union, namely, its Charter of Fundamental Rights.

The Court rejected the argument that the DSK had the degree of independence required by the Directive since it already satisfied the condition of independence for it to qualify as a court or tribunal of a Member State, and ruled that the words 'with complete independence' in the Directive must be given an autonomous interpretation, and in particular, that the supervisory authorities for the protection of personal data must enjoy an independence which allows them to perform their duties free from external influence, direct or indirect, which is liable to have an effect on their decisions.

The Court found that, irrespective of the federal authority to which the managing member of the DSK belonged, there was a service-related link between the managing member and the federal authority which allowed the activities of the managing member to be supervised by his hierarchical superior with extensive power of supervision over the officials in his department, enabling the hierarchical superior not only to ensure that his staff carried out their tasks in accordance with the law, efficiently and economically, but also to guide them in carrying out their duties, rectify any faults and omissions and ensure that working hours were adhered to, encouraging the promotion of his staff in accordance with their performance, and direct them to those tasks which best corresponded to their capacities.

Even if Austrian law was designed to prevent the hierarchical superior from issuing instructions to the managing member of the DSK, the fact remains that this law conferred on the hierarchical superior a power of supervision that is liable to hinder the DSK's operational independence.

On the second ground, the Court observed that although the DSK need not have a separate budget in order to be able to satisfy the criterion of independence, the attribution of the necessary equipment and staff to such authorities must not prevent them from acting 'with complete independence' in exercising the functions entrusted to them, and the staffing of the DSK with officials of the Federal Chancellery who are subject to supervision by the Federal Chancellery was not compatible with the requirement of independence.

The fact that the DSK was composed of officials of the Federal Chancellery, which itself was subject to supervision by the DSK, carried a risk of influence over the decisions of the DSK. Such an organisational overlap between the DSK and the Federal Chancellery prevented the DSK from being above all suspicion of partiality and was therefore incompatible with the requirement of 'independence'.

Finally, the Court found that the right of the Federal Chancellor to be informed at all times by the chairman and the managing member of all aspects of the work of the DSK was liable to subject the DSK to indirect influence from the Federal Chancellor, and this was incompatible with the criterion of independence, precluding the DSK from being capable of being regarded as operating, in all circumstances, above all suspicion of partiality.

The court ruled that by failing to take all of the measures necessary to ensure that the legislation in force in Austria meets the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), more specifically by laying down a regulatory framework under which the managing member of the Datenschutzkommission is a federal official subject to supervision, the office of the Datenschutzkommission is integrated with the departments of the Federal Chancellery, and the Federal Chancellor has an unconditional right to information covering all aspects of the work of the Datenschutzkommission, the Republic of Austria had failed to fulfil its obligations under the second subparagraph of Article 28(1) 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.

3.3. EUROPEAN DATA PROTECTION SUPERVISOR

A: Summary of activities and news:

In the course of 2012, the EDPS once again 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 his new enforcement policy: most EU institutions and bodies, including many agencies, are making good progress in complying with the Data Protection Regulation, while others should still increase their efforts.

In the consultation of new legislative measures, the EDPS issued a record number of opinions on a range of subjects. The Review of the EU legal framework for data protection was at the top of the EDPS agenda. However, the implementation of the Stockholm programme in the area of freedom, security and justice and the Digital Agenda, as well as issues in the internal market, such as financial sector reform, and in public health and consumer affairs, also had an impact on data protection. The EDPS also increased his cooperation with other supervisory authorities.

Special efforts were made in improving the efficiency and effectiveness of the EDPS organisation at a time of austerity. In this context, the EDPS completed a thorough Strategic Review, resulting in clear objectives for 2013-14 and internal Rules of Procedure covering all EDPS activities and the adoption of an Annual Management Plan.

Organisation	European Data Protection Supervisor (EDPS)
Chair and/or College	Peter Hustinx, Supervisor Giovanni Buttarelli, Assistant Supervisor
Budget	EUR 7 624 090
Staff	58 (all categories of staff included)
General Activity	
Decisions, opinions, recommendations	33 legislative opinions issued on, among others, initiatives relating to the Area of Freedom, Security and Justice, technological developments, international cooperation, data transfers and internal market. 15 sets of formal comments issued on, among others, intellectual property rights, civil aviation security, EU criminal policy, the Terrorist Finance Tracking System, energy efficiency and the Rights and Citizenship Programme. 37 sets of informal comments
Notifications	119 notifications of processing operations received from the Data Protection Officers of EU institutions and bodies for prior checking
Prior checks	71 prior-check opinions adopted notably on health data, staff

	evaluation, recruitment, suspicion and offences, and e-monitoring. 11 non prior-check opinions adopted.
Requests from data subjects	116 requests for information and advice from the public or interested parties included enquiries on the EU data protection legislation and its review, cloud computing, ACTA, eHealth, cookies and ePrivacy, biometrics, consent, large-scale IT systems such as SIS and EURODAC and data protection issues within the EU administration such as processing activities by EU institutions, bodies and agencies.
Complaints from data subjects	86 complaints received, 40 admissible Main types of violations alleged: access to and rectification of data, objection and deletion, excessive collection of data, transfer of data, data quality and information to data subjects, data security or disclosure of data.
Advice requested by parliament or government	The majority of the 33 legislative opinions mentioned above were issued upon the request of the European Commission (Article 28(2) of Regulation (EC) No 45/2001).
Other relevant general activity information	27 consultations on administrative measures related to the processing of personal data in the EU administration. Advice was given on a wide range of legal aspects related to the processing of personal data conducted by the EU institutions and bodies.
Inspection Activities	
Inspections, investigations	15 on-the-spot inspections and 6 visits carried out.
Sanction Activities	N/A
DPOs	
Figures on DPOs	58 DPOs in EU institutions, bodies and agencies

B. Information on case-law

EDPS participation in court proceedings

In 2012, the EDPS intervened in four cases before the Court of Justice of the EU and the Civil Service Tribunal.

The first case dealt with the alleged lack of independence of the Austrian data protection authority (DSK). The EDPS supported the position of the Commission which argued that the functional independence of the DSK provided for by Austrian law was not sufficient. The Court followed this reasoning and concluded that its close ties with the Austrian Federal Chancellery prevented the DSK from being above all suspicion of partiality.

The second case in which the EDPS intervened on the side of the applicant was *Egan and Hackett* v *European Parliament* (Case T-190/10). This was the last of three cases in which the General Court had to

rule on the relationship between the public access to documents regulation and the data protection regulation after the leading ruling in *Bavarian Lager* v *Commission* of 29 June 2010 (Case C-28/08 P). As in the other two cases, the EDPS argued in favour of greater transparency.

The EDPS intervened in two other cases which are still pending at the time of writing. The first case concerned an infringement proceeding against Hungary on the independence of the data protection authority. The second case, before the Civil Service Tribunal, concerned an alleged breach of the EU data protection Regulation (EC) No 45/2001 during an internal harassment investigation by the EIB.

The EDPS also closely followed several other cases without intervening such as the Spanish Google case which centres on the applicability of Spanish law implementing the European data protection Directive with regard to Google activities and two other cases related to the validity of the European data retention directive.

C. Other important information

Review of the EU Data Protection Framework

The major legislative project of 2012 for the EDPS was, without doubt, the data protection reform package. The EDPS underlined the need for updated and stronger EU rules on data protection on numerous occasions and on 25 January, the Commission adopted its reform package, comprising two legislative proposals: a general Regulation on data protection and a specific Directive on data protection in the area of police and justice.

The EDPS's first reaction was to welcome the general Regulation as a huge step forward for data protection in Europe, an excellent starting point for the adoption of European rules on data protection, robust enough to face future information technology-driven challenges.

However, with regard to the Directive, the EDPS was very critical of its inadequate content. He pointed out that the Commission had not lived up to its promises to ensure a robust system for data protection in the areas of police and justice and questioned why the Commission excluded the area from its original intention of proposing a comprehensive legislative framework.

On 7 March, the EDPS adopted an opinion elaborating his position on both proposals in greater detail. In a public statement, the EDPS concluded that the two legislative proposals would still leave Europe far removed from a comprehensive set of data protection rules — both at national and EU level — in all areas of EU policy. This is especially so because the proposals leave many existing EU data protection instruments untouched, such as the data protection rules for the EU institutions and bodies as well as specific law enforcement instruments.

One specific improvement of the proposed Directive was welcomed, namely that the proposal also covers domestic processing. However, the EDPS emphasised that this would only have added value if the Directive substantially increased the level of data protection in this area, which is not the case.

The EDPS highlighted that the proposed data protection rules for law enforcement were unacceptably weak. He noted many instances where departing from the rules provided for in the proposed Regulation was not justified. He pointed out that specific rules are needed for law enforcement, but not a general lowering of the level of data protection.

The EDPS also expressed particular concerns with regard to:

- the lack of legal certainty about the further use of personal information by law enforcement authorities;
- the lack of a general duty for law enforcement authorities to demonstrate compliance with data protection requirements;

- the weak conditions for transfers to third countries;
- the unduly limited powers of supervisory authorities.

Throughout the year, the EDPS delivered various speeches elaborating his position on the reform package and took part in topical discussions. He has remained available to the EU legislator for further advice or explanation of our position. In addition, through his participation in the Article 29 Working Party, the EDPS gave input on several, more specific issues.

The EDPS also made efforts to foster further discussion. In September and November, in close cooperation with the Europäische Rechtsakademie (ERA), the EDPS organised two seminars dedicated to the proposals. The seminars brought together many experts from national administrations, data protection authorities, EU institutions, academia, third countries and the private sector. The EDPS also launched a web page dedicated to the reform process, containing all relevant documentation, which is accessible via a link on his website.

Chapter Four

Principal Developments in EEA Countries

ICELAND

A. Summary of activities and news:

In early 2012 the National Directorate of Health demanded information from plastic surgeons on all women who had breast implants inserted since the beginning of the year 2000. The reason for this was a revelation of law breaches in the manufacturing of a brand of breast implants called PIP. The Icelandic Physicians Union, which was opposed to the information request, asked for guidance from the DPA on whether or not it was lawful to send personal information relating to the data subjects in question to the National Directorate of Health, including their diagnoses and identities. The purpose for the Directorate's planned collection of the data was, amongst other things, to be able to reach out to women with PIP breast implants and observe whether they went regularly to breast cancer checks, and to compare statistical health differences between women with PIP breast implants and women with other kinds of breast implants. However, according to the Icelandic Physicians Union, many women had expressed their concern on their information being sent. Furthermore, the Union stated that women with PIP breast implants had already been sent a letter from the relevant plastic surgeon, outlining the issue. The DPA gave guidance in two separate opinions, one given in April concerning data on women with PIP implants and the other given in March on women with other kinds of implants. The conclusion in both opinions was that the National Directorate of Health lacked legal authority to call for the information in question and, therefore, that the plastic surgeons were not permitted to give away the data without the data subjects' consent.

Another noteworthy case in 2012 regarded the Debtors' Ombudsman's dissemination of personal data on individuals in financial distress. The Ombudsman represents the interests of debtors, in part by facilitating agreements with creditors on debt mitigation. In the course of this task, an e-mail was sent from the Ombudsman to four pension funds, all of which are creditors of real estate loans, and — by mistake — to the National Hospital. Enclosed in the e-mail was a list of roughly 3 000 clients of the Ombudsman. The reason for the transmission of this list was to ask the pension funds whether or not individuals on the list had benefited from a certain debt-reducing measure. One of the pension funds had concerns regarding this transmission of data and alerted the DPA, which investigated the case. The DPA found that the office of the Ombudsman is, according to law, entitled to ask for information on whether its clients have benefited from the measure in question. However, the DPA stressed that when collecting information, the office of the Ombudsman is not legally authorised to transmit extensive lists of individuals who have asked for its assistance, only because the receivers of the list may possibly have relevant information on some of those individuals. Accordingly, the DPA came to the conclusion that the transmission of the list was in breach of the Data Protection Act. Furthermore, the DPA ordered the office of the Ombudsman to produce a written description of the security management system of its processing of personal data.

Organisation	Data Protection Authority
Chair and/or College	Mrs Sigrún Jóhannesdóttir, Commissioner; Mrs Björg Thorarensen, Chairman of the Board of Directors.
Budget	ISK 60 176 567 (equivalent to EUR 353 418 at the official exchange rate on 31 December 2012).
Staff	Five lawyers, one secretary.
General Activity	

Decisions, opinions, recommendations	150 (approx.)
Notifications	551
Prior checks	133 processing permits were granted.
Requests from data subjects	500 (approx.)
Complaints from data subjects	111
Advice requested by parliament or government	50 (approx.)
Other relevant general activity information	In all, 1 489 new cases were registered in 2012.
Inspection Activities	
Inspections, investigations	3
Sanction Activities	
Sanctions	With the exception of daily fines, i.e. fines imposed for each day that the DPA's orders are not obeyed, the DPA does not have the power to issue penalties or sanctions. Daily fines were not imposed in 2011.
Penalties	With the exception of daily fines, i.e. fines imposed for each day that the DPA's orders are not obeyed, the DPA does not have the power to issue penalties or sanctions. Daily fines were not imposed in 2011.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

On 27 August 2012, in Case 562/2012, the Supreme Court of Iceland overturned an order issued by a lower court, whereby wireless telephone providers that provide service in the Westman Islands were compelled to provide police with information on all incoming and outgoing telephone calls served through specific cell towers during a 10-minute interval on the morning of 6 August 2012. The court order had been issued in connection with a police investigation of a sexual offence that was allegedly perpetrated during that time period near the cell towers in question. At that time, a suspect in the case was observed, on a recording from a video surveillance system, running from the scene while talking on a cell phone. Article 80 of the Act on Criminal Procedure provides for police the authority to ask for information from telecommunications companies 'on telephone calls or other telecommunications with a specific telephone, computer or other kind of telecommunications device'. The Supreme Court found that since this provision is an exception to the right of privacy provided for in Article 71 of the Constitution, it

cannot be interpreted more broadly than the literal text provides for. Therefore, since the request for the court order does not identify information relating to a specific telephone, it must be declined.

LIECHTENSTEIN

A. Summary of activities and news

In 2012 the Data Protection Act (DSG) had been in force for ten years. To mark this, a representative survey among the population was commissioned. This was based on the Eurobarometer 225 from 2008. In summary, the following conclusions can be drawn: People have great confidence in public institutions and legislation in particular. However, this is qualified by the fact that 70 % of the population say that they only know a little about data protection. From the perspective of the Data Protection Office (Datenschutzstelle, DSS), the survey shows that the people should be better informed. The survey also shows — not surprisingly — that young people are only poorly informed and that, although people are aware of their rights, the number who knew about the right to information was smaller, compared to the right of deletion or correction. This is actually paradoxical, because a right of deletion can only be asserted if one knows what data is being processed, and one can only find this out through the right of information. The most conspicuous thing, in our opinion, was that only 40 % knew that there is a general entitlement to compensation; 42 % thought there was not. The general Data Protection Directive 95/46/EC provides for such an entitlement, which has not been incorporated into the DSG in Liechtenstein but applies nevertheless. Finally, around 28 % said that knew there was an independent data protection authority. Of these 28 %, only 15 % said they had ever had contact with it. This may be because, as a result of the high levels of trust mentioned above, there is no reason to contact it; another reason may be that there is simply insufficient awareness and a possible problem has not been identified; a third possible reason may be ignorance of the possibility of compensation. Details can be found in the Activity Report 2012.

A change to the DSG entered into force at the beginning of October. The main object of the change was the transposition of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Consequently, the restriction on the application of the DSG to pending criminal cases was removed, and data protection provisions were incorporated into the Code of Criminal Procedure. In addition, the provision on prior information was expanded and amended to reflect Directive 95/46/EC. At the request of the EFTA Surveillance Authority, the provision regarding the obligation on companies to notify sets of data was extended.

A public event was again held with the University of Liechtenstein on European Data Protection Day. The theme of the event was: "What does the internet know about me?" My data as a marketable commodity. The issue of online targeting was examined.

In today's society, anonymisation is an important measure to protect personal data. Pseudonymisation is also important. A guideline has been developed and published on both these topics.

Organisation	Data Protection Office
Chair and/or College	Philipp Mittelberger
Budget	EUR 596,000
Staff	2.3 Law, 1.0 Technology, 0.8 Administration
General Activity	
Decisions, opinions, recommendations	9 Responses to draft legislation ([17]) 4 Authorisations for video surveillance systems

(17) Cf. Activity report 2012 from the Data Protection Office under No. 3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

Notifications	By the end of the year, a total of 384 sets of data were listed in the register (a decrease from last year, due mainly to the appointment of data protection officers by authorities and private organisations, as a result of which they were exempt from the duty of notification).
Prior checks	N/A
Requests from data subjects	89 Requests from private individuals
Complaints from data subjects	N/A
Advice requested by parliament or government	None
Other relevant general activity information	640 Requests ([18]) (incl. private individuals, see above)
Inspection Activities	
Inspections, investigations	3 Inspections completed
Sanction Activities	
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	50 Data protection officers

B. Information on case-law

Nothing to mention.

(18) See request statistics from the Data Protection Office, under No. 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

NORWAY

A. Summary of activities and news

New strategies

As a follow-up to the strategy in the health sector, we continued to develop strategies for the justice and police sector and our international commitment. Furthermore, we have directed more attention to how we conduct our supervision, and administrative procedures.

In 2012, we increased the number of audits by 20 per cent, improved handling of individual cases and professionalised our counselling service.

Aftermath of the attack on 22 July 2011

In the reviews of several of the Ministry of Justice's proposals for legislative actions have been fierce and justified, and we noted that we must not lose our heads after the tragic events of 22 July 2011. It has also been important for us to communicate that the DPA wants to be a team player in solving future challenges by knowledge of new technology and community development.

New website

A key strategic priority is to enable the individual citizen to safeguard their personal privacy. One of the main measures to accomplish this was the launch of our new website. The philosophy behind the design is help to help yourselves and good information to citizens and controllers.

Organisation	Norwegian Data Protection Authority
Chair and/or College	Director Bjørn Erik Thon
Budget	NOK 36 million
Staff	41
General Activity	
Decisions, opinions, recommendations	
Notifications	2 954 new registered, total active 10 909. (We had at the end of the year over 2 000 notifications yet to register so the number of new notifications should be higher.)
Prior checks	132
Requests from data subjects	In total, the Norwegian DPA received 4 675 phone calls and 2 175 e-mails to our counselling service.
Complaints from data subjects	N/A
Advice requested by parliament	We received 105 invitations to comment on new legislation and

or government	sent in comments on 58 occasions.
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	Telecommunications, Internet and DLD - 7 Workplace - 10 Financial sector - 6 Health sector - 5 Justice and police - 2 Public Sector - 13 Camera - 4 Information security - 4 Re-audits - 4 Total - 55
Sanction Activities	
Sanctions	7 penalty fees, and 2 coercive fees, all by the DPA
Penalties	Penalty fees total NOK 1 300 000, coercive fees NOK 49 000
DPOs	
Figures on DPOs	203 DPOs representing a total of 390 firms and public offices.

B. Information on case-law

We have had many different rulings in 2012, and here we present some of the more important ones.

GE case — unauthorised disclosure of health information

The DPA received in March 2012 knowledge of the unauthorised disclosure of health information from multiple businesses (data controllers) to the supplier GE Healthcare Systems (GE) in the United States. We suspect that information on a substantial number of patients was retrieved and transferred to GE, including patients' names, ID numbers and date of birth and health data. The discrepancy came from eleven businesses in Norway. The initial information stated that there was information on 126 344 patients, but this figure is somewhat uncertain.

The hospitals in question had an agreement with the provider GE to operate, maintain and monitor equipment. The connection had been set up in such a way that GE was able to retrieve health information without any barriers.

In our ruling, we state that those data controllers must establish adequate safeguards to secure confidentiality and that the affected patients should be informed of the incident.

The Nettby case

The DPA decided in 2011 on the deletion of personal information originating from the closed social networking site Nettby (owned by the newspaper VG, one of the largest tabloids in Norway). VG challenged the decision and the Privacy Appeals Board determined the case. They stated that there is a

mandatory duty to deposit some of the 'documents' — information — that VG wanted to preserve to the National Library, i.e. the contents of the open forums and the parts that were open for indexing in search engines. The decision also applies to information that was not open for indexing but was available to all members of Nettby. Before deleting the information, VG had to meet this legal obligation.

The decision is important considering that many people use social networking sites. The public probably thinks that they to a small extent can decide how long information will be stored and who will gain access, both in the present and in the future.

The Appeals Board finds that everyone who makes available such a platform as Nettby has duties to deposit 'documents' to the National Library.

C. Other important information

Paper on electronic tracking in the workplace

In 2012, the DPA prepared a report, A normal day at work — electronic tracking in the workplace. The purpose was to illustrate how personal information is collected and used in everyday working life, and to increase knowledge and awareness. In this report, we looked at the workday for three different professions; bus drivers, home nurses and case handlers. We conducted interviews with representatives of management and employees at two jobs in each of the three selected occupational groups.

Chapter Five

Members and Observers of the Article 29 Data Protection Working Party

MEMBERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2012

Austria	Belgium
Mrs Eva Souhrada-Kirchmayer Austrian Data Protection Commission (Datenschutzkommission) Hohenstaufengasse 3 - AT - 1014 Wien Tel: +43 1 531 15 / 202525 Fax: +43 1 531 15 /202690 E-mail: dsk@dsk.gv.at Website: http://www.dsb.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 de la Presse, 35 -1000 Bruxelles Tel: +32(0)2/274 48 00 Fax: +32(0)2/274 48 35 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. BG- 1431 Sofia Tel+359 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg, kzld@cpdp.bg Website: http://www.cpdp.bg/	Mr Yiannos Danielides 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) 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/	Mrs Janni Christoffersen Danish Data Protection Agency (Datatilsynet) 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) Ratapihantie 9, 6rd floor - FI - 00251 Helsinki (P.O. Box 800) Tel: +358 295 666 700 Fax: +358 295 666 735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
France	**Germany**
Mrs Isabelle Falque Pierrotin 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 E-mail: Ifalquepierrotin@cnil.fr Website: http://www.cnil.fr	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) 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 Petros Christoforos 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: p.christoforos@dpa.gr Website: http://www.dpa.gr	Mr Dr Attila Péterfalvi President National Authority for Data Protection and Freedom of Information of Hungary (Nemzeti Adatvédelmi és Információszabadság Hatóság) Szilágyi Erzsébet fasor 22/c - HU - 1125 Budapest Tel:+36 1 391 1400 Fax: +36 1 391 1410 E-mail: ugyfelszolgalat@naih.hu Website: www.naih.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 Antonello Soro 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, a.soro@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 Tel: + 371 67223131 Fax + 371 67223556 E-mail: info@dvi.gov.lv Website: www.dvi.gov.lv	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) 1, avenue du Rock'n'Roll, L - 4361 Esch-sur-Alzette 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) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ The Hague Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl / international@cbpweb.nl Website: http://www.cbpweb.nl http://www.mijnprivacy.nl	Mr Wojciech Rafał Wiewiórowski Inspector General for Personal Data Protection (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw 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**
Mrs Filipa Calvão 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) Bd. Gral. Ghe. Magheru 28-30, 5ty floor, room 5, 1st district, postal code 010336, RO - Bucharest Tel: +40 31 805 9211 Fax: +40 31 805 9602 E-mail: international@dataprotection.ro;

	anspdcp@dataprotection.ro Website: www.dataprotection.ro
Slovakia	**Slovenia**
Mrs Eleonóra Kročianová Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky) Hraničná 12 - SK - 82007 Bratislava 27 Tel: +421 2 323 132 11 Fax: +421 2 323 132 34 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	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: gp.ip@ip-rs.si Website: http://www.ip-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	Mrs Kristina Svahn Starrsjö Data Inspection Board (Datainspektionen) Drottninggatan 29, 5th floor Box 8114 - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@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: www.ico.org.uk	Mr Peter Hustinx European Data Protection Supervisor — EDPS Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 30, BE - 1000 Brussels Tel: +32 2 283 1915 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: www.edps.europa.eu

OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2012

Iceland	Norway
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 Kim Ellertsen The Norwegian Data Protection Autority (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
Liechtenstein	**Republic of Croatia**
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	Mr Dubravko Bilić Director Mrs Sanja Vuk Head of department for EU and Legal Affairs Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka - AZOP) Martićeva 14. 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 Article 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

DS-AA-15-001-EN-N

Publications Office

doi: 10.2838/83967