



Seventeenth Report

of the Article 29 Working
Party on Data Protection

Covering the year 2013

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

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

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

**Seventeenth Report of the Article 29 Working Party on Data Protection
— Covering the year 2013**

European Commission
Directorate-General for Justice and Consumers
1049 Brussels
BELGIUM

PDF ISBN 978-92-79-52066-2 ISSN 2363-099X doi:10.2838/244921 DS-AA-15-002-EN-N

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

Luxembourg: Publications Office of the European Union, 2016

© European Union, 2016
Reproduction is authorised provided the source is acknowledged.

Cover image: © robu_s / Fotolia.com

Seventeenth Report of the Article 29 Working Party on Data Protection

Covering the year 2013

Contents

INTRODUCTION BY THE CHAIRMAN	2
ISSUES ADDRESSED BY THE ARTICLE 29 DATA PROTECTION WORKING PARTY	3
MAIN DEVELOPMENTS IN MEMBER STATES	15
AUSTRIA.....	16
BELGIUM	19
BULGARIA	24
CROATIA.....	31
CYPRUS	33
CZECH REPUBLIC.....	35
DENMARK	38
ESTONIA	41
FINLAND	45
FRANCE	49
GERMANY.....	57
GREECE.....	61
HUNGARY.....	67
IRELAND.....	73
ITALY	75
LATVIA	81
LITHUANIA.....	83
LUXEMBOURG	86
MALTA	89
NETHERLANDS.....	92
POLAND	96
PORTUGAL.....	102
ROMANIA.....	104
SLOVAKIA.....	107
SLOVENIA	111
SPAIN	119
SWEDEN	122
UNITED KINGDOM.....	125
EUROPEAN UNION AND COMMUNITY ACTIVITIES.....	129
3.1. EUROPEAN PARLIAMENT	130
3.2. EUROPEAN COMMISSION.....	131
3.3. EUROPEAN COURT OF JUSTICE.....	136
3.4. EUROPEAN DATA PROTECTION SUPERVISOR.....	138

MAIN DEVELOPMENTS IN EEA COUNTRIES	143
ICELAND.....	144
LIECHTENSTEIN.....	147
NORWAY.....	149
MEMBERS AND OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WP	152
MEMBERS OF THE ART. 29 DATA PROTECTION WP IN 2013.....	153
OBSERVERS OF THE ART. 29 DATA PROTECTION WP IN 2013	158

INTRODUCTION BY THE CHAIRMAN

After the presentation of the proposals for a new legal framework in the European Union (EU) on data protection in January 2012, the Article 29 Working Party has followed the reform closely and provided input on several issues in 2013, such as on the concepts of consent, legitimate interest, purpose limitation, and profiling.

While, at the time of writing this foreword, the European Parliament has already adopted its position on the package, the Council continues to have discussions in regard to the same. Nevertheless, with the new Commission's mission statement in mind, expectations are high that the negotiations between the legislators in the EU will commence soon.

The reform of the EU data protection legal framework was naturally one of the main issues that the Working Party focussed on in 2013, but it was certainly not the only topic that needed attention from the EU data protection authorities. When Edward Snowden revealed in the summer of 2013 that the NSA was conducting large-scale, indiscriminate surveillance activities, accessing all (personal) data that was held or passed through US-based firms or soil, the whole world responded with disbelief and anger.

The extremity of these revelations sparked public outrage and a critical dialogue between the EU and the US ensued, in which the Working Party and national EU DPAs were also involved. The amount and manner in which the personal data of European citizens was accessed by the intelligence services of another country, an ally, led the Working Party to request that the European Commission engage with the US authorities to address the situation.

Furthermore, the Working Party adopted an opinion addressing the key data protection risks of mobile apps, detailing the specific obligations under EU law of app developers and all other parties involved in the development and distribution of apps. Special attention was paid to apps targeting children.

In 2013, the Working Party also issued an opinion on purpose limitation in which it made clear that further processing for a different purpose than for which the personal data were originally collected, does not necessarily mean that it is incompatible, but compatibility needs to be assessed on a case-by-case basis. In its opinion, the Working Party offers guidance on the application of the principle under the current legal framework; however, it also, in response to the discussions taking place regarding the principle of purpose limitation in the review process, provides recommendations for the future general data protection legal framework.

Last, but not least, the consideration of data protection is not an EU-only issue, and the WP29 has stayed in contact with its counterparts from all over the world. The protection of personal data is a common goal and is increasingly a global issue. Only through cooperation, both between ourselves and with others around the world, will we be able to ensure adequate protection globally.

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 Binding Corporate Rules (BCR)

19.4.2013 [Explanatory Document on the Processor Binding Corporate Rules](#) - WP 204

This document aims to provide guidance on the application of Article 26 (2) of the Directive 95/46/EC in the case of BCR for Processors (Processor to sub-processor within the same corporate group), which came into use on 1 January 2013, as well as simplification for multinational organisations routinely processing and exchanging personal data on behalf of controllers on a world-wide basis. This working document should be regarded as a first step to highlight the possibility to use BCR for Processors on the basis of a self-regulatory approach and co-operation among the authorities, without prejudice to the possibility to use other tools for the transfer of personal data abroad, such as standard contractual clauses or the Safe Harbour principles where applicable.

1.1.2 Overseas transfers for specific purposes

4.4.2013 [Letter from the Article 29 Working Party addressed to Mr López Aguilar, Committee on Civil Liberties, Justice and Home Affairs, European Parliament, regarding the proposal for a new Anti-Money Laundering/Counter Terrorist Financing \(AML/CFT\) Directive](#)

In this letter the Working Party sets out to the relevant European Parliament committee its concerns regarding the AML/CFT legislation. The Working Party considers, *inter alia*, that the provision relating to the prohibition of tipping off constitutes an arbitrary limitation of the rights of access and rectification, and recommends the specification of which processing operations fall outside the prohibition, and obliges national regulators and the industry to make the necessary adjustments.

The Working Party also advocates clarifying the conditions legitimising transfers of personal data for AML/CFT purposes to third countries which do not ensure an adequate level of data protection. Member states should specify which important public interests apply to the transfer of the data in question to the country in question, and what guarantees are in place to ensure effective data protection.

The Working Party advises more specific modalities and/or appropriate safeguards be added to every profiling operation, such as CDD, and encourages stakeholders to improve cooperation in the area of data protection, either by a reference to the requirement of prior checking as laid down in article 20 of Directive 95/46/EC, or a reference to the requirement of a privacy impact assessment in article 33 of the draft regulation.

13.6.2013 [Final uniform application procedure and standard templates for citizens](#)

The Working Party, in conjunction with US authorities, has developed a standard application for access to and/or rectification, erasure, or blocking of personal data held pursuant to the US Terrorist Finance Tracking Program (TFTP) Procedure for data protection authorities, including the detailed uniform procedure following a data subject's request for access, rectification, erasure, or blocking of personal data.

11.7.2013 [Letter addressed to Ms. Cecilia Malmström, Commissioner for Home Affairs regarding Advance Passenger Information \(API\)](#)

This request by the Working Party to the Commission is in response to the requirement that air carriers in the EU provide advance passenger information (API) to the authorities of the third countries which are the destinations of the relevant flights. The Working Party is not sure that there is a current legal basis for such transfer, even if the data sought is what would be provided by the passengers when entering the destination country in any event, and therefore, in order to remove legal uncertainty and ensure consistency, asks that the European Commission takes steps to introduce a specific legal basis.

This legal basis should provide that data should be collected and transferred only if required under the laws of the country of destination; they should be collected and transferred by the airlines upon check-in only for the purpose of fulfilling border control obligations of the third country, and be deleted without delay once the aircraft has reached its final destination; the scope of transferred data should be limited to the information contained in the Machine Readable Zone of the passport or another travel document; biometric data should not be transferred; passengers should be informed of the transfer before purchasing their ticket, and also when their data are collected.

The legal basis should also provide for adequate safeguards for data subjects, including modalities to exercise their rights, and could be introduced during the evaluation and revision of Directive 2004/82/EC.

9.10.2013 [Letter from the A29 WP Chairman Jacob Kohnstamm to the Members of the LIBE Committee regarding the Proposal for Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data](#)

The letter sets out the Working Party's views on the EU-Canada PNR agreement. The Working Party regards data minimisation as being of primary importance for the privacy of passengers, and recommends that the necessity of each item in the list of data be reviewed separately from the Canadian side. The Working Party also advises re-examining the definitions of prevention, detection, investigation, and prosecution of terrorist offences or serious transnational crime, because they are too vague.

The Working Party regrets that the Agreement allows the processing of sensitive data by the Canadian authorities, and recommends that, in the case of data breaches or data protection incidents, the relevant EU data protection authorities should be informed.

The Working Party makes suggestions regarding oversight of the implementation of the Agreement, and also recommends that the parties request air carriers to provide to passengers information in regard to the reasons, purpose, use, right of access, right of information, right of correction, and redress relating to the processing of their personal data.

The Working Party suggests much more detailed reference to access and redress, and disagrees with the extension of the retention period by comparison with the 2005 agreement. It also suggests that the authorities to which the data may be transferred be listed in the agreement or its annex.

8.11.2013 [Second letter from the Article 29 Working Party addressed to Mr López Aguilar, Committee on Civil Liberties, Justice and Home Affairs, European Parliament, regarding the proposal for a new Anti-Money Laundering/Counter Terrorist Financing \(AML/CFT\) Directive](#)

By letter dated 8 November 2013, the Working Party followed up this letter reiterating the concerns set out previously, which had not yet been taken into account by the co-legislators, *inter alia*, that the proposals were not specific enough to be considered as providing a clear legal basis, they contained new

Chapter One Issues Addressed by the Article 29 Working Party

measures which not take into account privacy and data protection, and that they ignored cooperation with, and the role of, data protection authorities.

5.12.2013 - [Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdictions, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime](#)

The Council of Europe (COE) ad-hoc subgroup of the T-CY on jurisdiction and transborder access to data and data flows presented proposals to amend the Protocol to the Budapest Convention on Cybercrime to allow for additional possibilities for transborder access to data, including transborder access without consent.

The Working Party considers that, while the processing of data for law enforcement purposes is legitimate as long as it complies with the law, given the growing importance of cloud computing, along with the accompanying difficulty in linking data to a specific location, and the lack of control and transparency inherent in cloud computing data processing, law enforcement access to data in another jurisdiction is in breach of the data protection principles of necessity, proportionality, and purpose limitation.

Moreover, given that both COE Conventions 108 and 185 are international conventions, it means that, in the event of any incompatibility with the European Convention of Human Rights, only European states would be subject to the jurisdiction of the European Court of Human Rights, thereby allowing for non-compliance by non-COE states.

11.12.2013 [Letter from the Article 29 Working Party to the International Air Transport Association \(IATA\) on "New Distribution Capability"](#)

The Working Party wrote to IATA, setting out its preliminary observations on IATA's new distribution capability, informing them that the amount of personal data requested should be proportionate to the purpose of the processing, and that the processing should have a legal basis under article 7 of Directive 95/46/EC.

The Working Party was not sure that the proportionality test was being met, or that a legal basis based on the performance of a contract was applicable in the case of a general search request not limited to a specific airline. Processing can be based on consent given freely, unambiguously, and expressly.

Other issues to be taken into account include the role of the carriers themselves in the booking process, and whether they could be regarded as controllers in some circumstances in regard to data retention, information for the passengers, potential transfers to third countries outside EU, and the risk of profiling.

1.2 Electronic Communications, Internet, and New Technologies

27.2.2013 [Opinion 02/2013 on apps on smart devices](#) - WP 202

In this opinion, the Working Party clarifies the legal framework applicable to the processing of personal data in the development, distribution, and usage of apps on smart devices, with a focus on the consent requirement, the principles of purpose limitation and data minimisation, the need to take adequate security measures, the obligation to correctly inform end users, their rights, reasonable retention periods and, specifically, fair processing of data collected from and about children.

The opinion concludes that many types of data available on a smart mobile device are personal data. The relevant legal framework is Directive 95/46/EC, in combination with the specific consent requirement

Chapter One Issues Addressed by the Article 29 Working Party

in Article 5(3) of the ePrivacy directive. These rules apply to any app targeted to app users within the EU, regardless of the location of the app developer or app store.

The fragmented nature of the app ecosystem, the wide range of technical access possibilities to data stored in or generated by mobile devices and the lack of legal awareness amongst developers create a number of serious data protection risks for app users. These risks range from a lack of transparency and lack of awareness amongst app users to poor security measures, invalid consent mechanisms, a trend towards data maximisation and elasticity of data processing purposes.

There is an overlap of data protection responsibilities between the different parties involved in the development, distribution and technical capabilities of apps. Most conclusions and recommendations are aimed at app developers (in that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app), but often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem, such as the OS and device manufacturers, the app stores and third parties, such as analytics providers and advertising networks.

13.3.2013 [Letter from the A29 WP to Neelie Kroes, Vice-President of the European Commission, on the Commission's proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market](#)

This letter sets out the Working Party's data protection concerns about the European Commission's proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market. These concerns include the interpretation of certain terms used in the proposal, the use of pseudonyms, data minimisation and personal data included in certificates, the applicability of Directive 95/46/EC; electronic trust services and seals and mass signatures and qualified signatures for employees; electronic identity and data minimisation and the danger of profiling through online authentication and validation systems; and the security of electronic signatures, supervisory authorities, lists of qualified trust services, and security level definitions.

18.6.2013 [Letter addressed to Google regarding Google Glass, a type of wearable computer in the form of glasses](#)

The Working Party wrote to Google concerning Google Glass, expressing its concerns about its compliance with data protection laws; privacy safeguards; the information collected and whether this is further shared; the intended purpose of the information; facial recognition; the broader social and ethical issues raised, for example, by the surreptitious collection of information about other individuals, and the results of any privacy risk assessment.

2.10.2013 [Working Document 02/2013 providing guidance on obtaining consent for cookies](#) - WP 208

Since the adoption of the amended e-Privacy Directive 2002/58/EC in 2009, a range of practical implementations have been developed by websites in order to obtain consent for the use of cookies for various purposes. The range of consent mechanisms deployed by website operators reflects the diversity of organisations and their audience types. The website operator is free to use different means for achieving consent as long as this consent can be deemed as valid under EU legislation. This opinion assesses whether or not a particular solution implemented by the website operator fulfils all the requirements for valid consent.

In practice, the implementation of the legal requirements varies among website operators across EU Member States. Generally, they are based on a number of practices, none of which could, by itself, result in valid consent being given.

Given diverging interpretations of the Directive, the opinion provides further clarity on the requirements of valid consent and its main elements, namely:

Chapter One Issues Addressed by the Article 29 Working Party

1. Specific information - consent must be specific and based on appropriate information, so blanket consent without specifying the exact purpose of the processing is not acceptable.
2. Timing - consent must be given before the processing starts.
3. Active choice - the procedure to seek and to give consent must leave no doubt about the data subject's intention. There should be an active indication of the user's wishes.
4. Freely given - consent can only be valid if the data subject is able to exercise a real choice.
5. If website operators wish to ensure that a consent mechanism for cookies satisfies the conditions in each Member State, such a consent mechanism should include each of these elements.

1.3 REVISION OF THE DATA PROTECTION LEGAL FRAMEWORK

22.1.2013 [Working Document 01/2013 - Input on the proposed implementing acts](#) - WP 200

In this working document, the Working Party elaborates on the differences between delegated and implementing acts as indicated in Opinion 8/2012, lists the relevant criteria for determining the justification and need of implementing acts, and provides an article-by-article assessment of all possible implementing acts.

26.2.2013 [Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive](#) - WP 201

In this opinion, the Working Party sets out its comments on the draft Directive from the perspective of the use of data of non-suspects, the rights of data subjects, the use of privacy impact assessments in the law enforcement sector, and the powers of data protection authorities.

27.2.2013 [Statement of the Working Party on current discussions regarding the data protection reform package](#)

This statement, which follows the Working Party's opinions WP191 and WP 199, elaborates on previously expressed concerns in the areas of flexibility in the public sector; personal data and pseudonymisation; consent; governance; international transfers, and the risk-based approach. The issues of lead DPA and competence and of the exemption for household and personal activities are also more thoroughly discussed.

As regards flexibility in the public sector, the Working Party considers that a distinction between the public and private sectors would only lead to legal uncertainty. It would also be unworkable in practice on account of the differences from Member State to Member State regarding the nature and scope of the tasks performed by public bodies.

Pseudonymising data means disguising identities in a re-traceable way. Disguising identities in a way which renders re-identification impossible is anonymisation. However, when pseudonymisation or encryption is done in such a way as to enable an individual to be backtracked or (indirectly) identified, data protection rules continue to apply.

Wherever consent is relied upon as a legal ground, it must be sufficiently clear. It can be expressed in many different ways, but it should be an essential requirement that it is explicit. Imposing the burden of proving consent on the controller strengthens the rights of individuals.

Chapter One Issues Addressed by the Article 29 Working Party

The increased duties for the European Data Protection Board (EDPB) and EU data protection authorities will enhance the protection of personal data, although they raise the issue of adequate resources for the latter. In addition, they should be able to define their own priorities, and instigate actions such as investigations on their own initiative, notwithstanding the obligations regarding cooperation, mutual assistance, and consistency.

It is important that the personal data of EU individuals receives the same protection whether processed within the EU or transferred outside the EU. Non-binding instruments and self-assessment in the context of transfers to third countries should remain an exception available only in limited circumstances, and only for non-massive and non-repetitive transfers. In cases of disclosure not authorised by law, resorting to mutual legal assistance treaties should be mandatory.

Some of the provisions in the proposed Regulation imposing burdens on some controllers may be perceived as inequitable and should therefore be tailored to the controller and the processing operations concerned. Compliance should be about ensuring that personal data is sufficiently protected, and this may vary from controller to controller. This depends not only on the size of the controller or the volume of processing, but also on the nature of the processing and the categories of data.

Annex 1: [Proposals for Amendments regarding Competence & Lead Authority](#)

In this annex, the Working Party offers proposals for Amendments regarding competence and lead authority on the basis that all supervisory authorities must be competent on the territory of their Member State; the 'lead authority' must be the single contact point for a company, taking care of the decision-making procedure in which all involved supervisory authorities will take part; the outcome of the decision-making procedure should be binding for all supervisory authorities; the notion of main establishment should be clarified, and when ambiguity remains about which authority will be the 'lead authority', a decision-making procedure must be provided, preferably by the European Data Protection Board; and individuals must always have the option of seeking judicial redress in courts in their own Member State.

Annex 2: [Proposals for Amendments regarding exemptions for personal or household activities](#)

In this annex the Working Party offers proposals for amendments regarding exemptions for personal or household activities by reference to criteria for deciding whether processing is being done for personal or household purposes; other relevant elements of the law including libel, harassment, malicious communications, threatening behaviour incitement, and in some cases persecution, or discrimination; gainful interest; connection with a professional or commercial activity; personal processing and dissemination to the world at large; and correspondence and the keeping of addresses.

13.5.2013 [Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation](#)

In this document the Working Party presents its advice on the essential elements of a definition and a provision on profiling in the General Data Protection Regulation draft, commencing from the point of departure that the connection and linking of personal data in order to create profiles can have significant impacts on data protection. Profiling enables a person's personality or aspects of their personality to be determined, analysed, and predicted, frequently without the data subject's knowledge. As a result, data subjects may not be able to exercise sufficient control over the processing of their personal data.

The Working Party considers it necessary to include a definition of profiling in the General Data Protection Regulation, and offers a definition.

The Working Party favours a comprehensive approach to determine specific legal requirements, not only for the usage and further processing of personal data obtained by profiling, but also for the collection of profiling data itself and the creation of profiles as such, and suggests including additional elements such

as greater transparency and more individual control in regard to the decision on whether or not one's own personal data may be processed for the purpose of profiling; explicit consent as a legal basis for processing in the context of profiling, as well as the right to have access to, to modify, or to delete the profile information attributed to them, and a higher degree of responsibility and accountability on data controllers with respect to the use of profiling techniques.

Profiling should be subject to measures to safeguard the data subject's rights and freedoms, adopted on the basis of a data protection impact assessment, and should include data protection-friendly technologies and standard default settings, specific measures for data minimisation, and data security, as well as human intervention in defined cases.

Given that profiling may have different effects on individuals' privacy, the Regulation should provide clear rules on the lawfulness and conditions for the processing of personal data in the context of profiling, leaving some discretion in assessing the actual effects on data subjects of a specific type of processing. The Working Party therefore supports an approach which covers profiling based on it, only to the extent that they significantly affect the interests, rights, or freedoms of the data subject. The term "significantly affect" should be interpreted while taking into account the scope of the basic right to data protection, assessing the interests of controllers, and analysing the potential impacts of profiling technologies on the rights and freedoms of data subjects. This can best be done by the European Data Protection Board.

1.4. PERSONAL DATA

1.4.1 Purpose limitation

2.4.2013 [Opinion 03/2013 on purpose limitation](#) - WP 203

This opinion aims to analyse the principle of purpose limitation, provide guidance for the principle's practical application under the current legal framework, and formulate policy recommendations for the future. Purpose limitation protects data subjects by setting limits on how data controllers are able to use their data, while also offering some degree of flexibility for data controllers. Personal data must be collected for specified, explicit, and legitimate purposes (purpose specification) and not be further processed in a way incompatible with those purposes (compatible use).

Compatibility must be assessed on a case-by-case basis while taking into account all relevant circumstances, and with particular reference to the relationship between the purposes for which the personal data were collected and the purposes of further processing; the context in which the personal data were collected and the reasonable expectations of the data subjects as to their further use; the nature of the personal data and the impact of further processing on the data subjects, and the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The data controller cannot legitimise incompatible processing by relying on another legal ground in article 7 of Directive 95/46/EC. The purpose limitation principle can only be restricted by Article 13 of the Directive.

Article 6(4) of the proposed Data Protection Regulation provides a broad exception from the requirement of compatibility, which would severely restrict its applicability and risk, eroding this key principle. The Working Party therefore recommends that the proposed paragraph 4 be deleted, and that legislators adopt the above list of relevant factors in order to assess compatibility.

[Opinion 06/2013 on open data and public sector information \('PSI'\) re-use](#)  (416 kB)  - WP 207 (5.6.2013)

This opinion concerns the amended Directive 2003/98/EC on the re-use of public sector information (the 'PSI Directive'), which harmonized the conditions for re-use of public sector information, but left optional the decision whether or not to make data available for re-use.

The purpose of the amendment was to make all public information reusable for both commercial and non-commercial purposes, with exceptions, including data protection.

The amended Directive now obliges public bodies to permit re-use of all public information which is available to the public under national law, and always subject to data protection law.

Increased accessibility to public information comes with risks. To minimise these risks, in all cases where the protection of privacy and personal data is at stake, a balanced approach is needed between the development of the re-use market on the one hand, and the right to the protection of personal data and privacy on the other. The focus of open data is on the transparency and accountability of public sector bodies, and economic growth, not on the transparency of individual citizens. Rather than personal data, it is often statistical data derived from personal data that are and should be made available for re-use.

In some situations personal data can be re-used, where necessary, with legal, technical or organisational measures in place to protect the individuals concerned. In such cases a clear legal basis is necessary, taking into account the principles of proportionality, data minimisation, and purpose limitation.

The Working Party recommends that the possibility of information containing personal data should be taken into account at the earliest opportunity, in accordance with the principle of 'data protection by design and default'; data protection impact assessments should be conducted before allowing publication of personal data or anonymised data derived from personal data; when data are anonymised, it is essential to assess the risk of re-identification, and a good practice to carry out re-identification testing; the outcome of the assessment could help identify appropriate safeguards to minimise risks or lead to a decision to refrain from publication and/or making available for re-use; terms of any re-use licences should include a data protection clause; where the impact assessment concludes that a license does not address data protection risks, personal data should not be disclosed; where appropriate, public sector bodies should ensure that personal data are anonymised and license conditions specifically prohibit re-identification of individuals and re-use of personal data for purposes that may affect the data subjects; and Member States should consider establishing and providing support to knowledge networks/centres of excellence, thereby enabling the sharing of good practices related to anonymisation and open data.

6.6.2013 [Letter from the Article 29 Working Party addressed to ICANN regarding the statement on the data protection impact of the revision of the ICANN RAA](#)

In this letter the Working Party addresses the compliance of ICANN's final Registrar Accreditation Agreement (RAA) proposal with European data protection law, specifically addressing the legitimacy of the data retention obligation for registrars.



ICANN has included a procedure for registrars to request a waiver from these requirements, if necessary, to avoid a violation of applicable data protection law. Such a waiver request can be based on written guidance from a governmental body of competent jurisdiction providing that compliance with the data retention requirements violates applicable law.

The Working Party observed that the proposed new data retention requirement did not result from any legal requirement in Europe and suggested that, taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the data protection risks were disproportionately large compared to the benefits of the proposal.

Chapter One Issues Addressed by the Article 29 Working Party

The Working Party also objected to data retention based on a contract rather than on national law, for example, to address a pressing social in law enforcement. The fact that these personal data could be useful for law enforcement did not legitimise their retention after expiry of the contract.

1.4.2 Smart Grids

[Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems \('DPIA Template'\) prepared by Expert Group 2 of the Commission's Smart Grid Task Force](#)  (285 kB)  - WP 205 (22.4.2013)

In 2012, the European Commission issued a Recommendation on the preparation for the roll out of smart metering systems (the 'Commission Recommendation') to Member States for the rollout of smart metering systems in the electricity and gas markets, *inter alia*, for guidance on data protection considerations. It recommended data protection by design and by default and also provided that Member States should adopt and apply a template for a data protection impact assessment ('DPIA Template'), developed by the Commission and submitted to the Working Party for its opinion.

This is the Working Party's opinion, which concludes that, although improvements on the template have been made, further work is necessary on issues such as scope, stakeholders, legal basis and choice, data minimization, and privacy enhancing technologies.

1.4.3 Borders and Home Affairs

23.4.2013 [Letter from the Article 29 Working Party, addressed to IATA, regarding Checkpoint of the Future](#) and [Annex](#)

The Working Party wrote to IATA regarding its proposed Checkpoint of the Future, indicating that it raised fundamental questions about how it ensured compliance with EU data protection rules, and in particular, the principles of necessity and proportionality; data quality, data minimisation, and purpose limitation; special categories of data; legitimacy of processing; data subjects' rights and transparency; automated decisions and profiling; international transfers of personal data, and data security and confidentiality. Privacy by design should be a guiding principle, and privacy concerns should be taken into account from the outset.

The Annex to the letter set out specific questions on the topics of effectiveness; necessity, and proportionality; passenger differentiation; data controllership and compliance; purpose limitation; known traveller programmes; behavioural analysis; subject access and transparency; identity management; access to data and data sharing; and technology.

6.6.2013 [Opinion 05/2013 on Smart Borders](#) - WP 206

In 2013, the Commission presented proposals for an Entry Exit System (EES) and a Registered Traveller Programme (RTP) for the Schengen Area, collectively known as "Smart Borders". A proposal for necessary alterations to the Schengen Borders Code was also presented.

The Entry Exit System proposal proposes a centralised storage system for entry and exit data of third country nationals (TCNs) admitted for short stays to the Schengen area, whether they require a Schengen visa or not. Rather than having passports stamped on entry to and exit from the Schengen Area, data relating to the identity of the visitor and length and purpose of stay will be entered in the system on entry and will be checked on exit, to ensure that the TCN has not exceeded the maximum permissible stay. A centralised system means that the EES data can be checked no matter where the TCN exits the Schengen Area. The primary purpose of the system is to counteract the problem of overstay in the Schengen Area. The EES proposal is for a system initially based on personal data needed for the identification of persons (alphanumeric data), with biometric data to be introduced after three

Chapter One Issues Addressed by the Article 29 Working Party

years. After two years, there is to be an evaluation on whether law enforcement authorities and third countries should be given access to the system.

The RTP proposes a voluntary registered traveller programme for frequent travellers to the Schengen Area, for example, business visitors. TCNs may apply for registered traveller status and benefit from faster border crossings. The RTP will be based on a central repository containing biometric data and a token containing a unique identifier held by the traveller.

This opinion calls into question whether the EES can be effective in achieving its own stated aims. However, even if it were accepted that the EES provided significant added value, it has been concluded that the added value of the EES in achieving its stated aims does not meet the threshold of necessity which can justify interference with the rights under Article 8 – EU Charter. Furthermore, it has been expressed that the added value of the EES is not proportionate to the scale of its impact on fundamental rights in relation to each of its aims, and that alternatives exist to meet its aims.

9.12.2013 [Letter from the Article 29 Working Party to Mr López Aguilar, Committee on Civil Liberties, Justice and Home Affairs, European Parliament, regarding Proposal for a Regulation of the European Parliament and of the Council on EUROPOL](#)

In this letter the Working Party comments on the European Commission's Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol Regulation), in relation to which both the European Data Protection Supervisor (EDPS) and the Joint Supervisory Body of Europol (JSB Europol) have already adopted opinions.

The Working Party considers that the level of data protection as defined in the proposal falls short of the standards set out in the Europol Council Decision, and that the proposal needs to be improved in order to contribute to an improved and stronger data protection regime for Europol. Therefore, it seems to be necessary to reformulate some key provisions in the draft Europol Regulation and to introduce stronger data protection safeguards where possible, specific to Europol's activities.

The Working Party also considers that a more accurate definition is needed when describing the scope of Europol's competences as well as specific crimes where Europol will have competence in the future.

There is no clear allocation of responsibilities with regard to the information provided by third parties, nor is there any clear assignment of responsibilities related to the results of the analytical tasks carried out by Europol. Since there is a link between the data used for preparing a report and the final result, any report based on inaccurate data should be updated accordingly and this can only be done when a clear responsibility is allocated.

The provisions on the purposes of information processing activities do not seem to enable Europol to perform its present and intended future tasks, and will have a negative impact on individuals' privacy. The conditions for setting up data processing systems where only dedicated personal data should be processed should be defined. The proposal would benefit from the addition of specific elements of privacy by design, namely, the inclusion of privacy impact assessments as a mandatory tool in specific cases, as well as mechanisms ensuring privacy by default.

The Working Party notes the absence of an obligation to provide notification of personal data breaches to the supervisory authority and to the data subject in specific cases as included in the data protection package, notably Articles 28 and 29 of the proposed Directive. The Working Party recommends including this obligation in the proposal, taking into account the specificities of Europol's tasks.

1.4.4 Sport

5.3.2013 [Letter from the Article 29 Working Party addressed to the World Anti-Doping Agency, regarding 3rd stage of WADA's consultation in the context of the review of the World Anti-Doping Code and its International Standards and annex contribution](#)

Following its opinions WP156 and WP 162 in 2008 and 2009, respectively, on the Standard for the Protection of Privacy and Personal Information, on certain relevant provisions of the World Anti-Doping Code and the Standard on Testing, the Working Party monitored the revision process of both the World Anti-Doping Code, and with this letter, in the context of the third and final stage of the public consultation organised by WADA, expressed a number of observations and concerns relating principally the issues of legitimacy based on consent, the proportionality of location data, retention periods and (the terms for) the automatic publication of sanctions, as well as the adequacy of the framework for international data transfers.

1.4.5 Surveillance

18.4.2013 [Letter from the Article 29 Working Party addressed to INDECT](#)

The Working Party wrote to the project coordinator of INDECT, a Commission funded research project, in response to an explanation of the project INDECT provided to the Working Party the previous year. The Working Party clarified that, in many cases, video footage must be considered as personal data because of its special nature, and provided INDECT with a brief overview of what constitutes personal data.

The Working Party acknowledged that the INDECT project had obtained the consent of all individuals involved in the research, but suggested that when the research project involved the processing of personal data and was likely to affect the privacy of European citizens, not only the research itself and the way in which it is undertaken, but also the results of the research needed to be in line with the fundamental rights, and in particular with the right of privacy and data protection, before the results were deployed in practice.

The Working Party suggested proactive considerations such as “data minimisation”, “privacy by design”, and “data protection by default” principles in the development of new technologies and solutions, appreciating that many technologies aimed at detecting potential threats focused the attention of security or surveillance operators on possible dangerous events through “innovative human decision support algorithms” that do not need to identify the persons on the video footage.

The Working Party drew the attention of INDECT to privacy and data security risks that were associated with the nature of the research being conducted.

Chapter Two

Main Developments in Member States

AUSTRIA



A. New developments and activities

In the reporting period, Parliament passed the **Data Protection Act (DSG) Amendment 2014**². This requires a **monocratic Data Protection Authority** to be established to replace the Data Protection Commission. An appeal process from the Data Protection Authority to the Federal Administrative Court (itself new from 2014) is also envisaged.

The Data Protection Commission therefore ceased its activity as supervisory authority for data protection as defined in Article 28 of the Data Protection Directive³ on 31.12.2013.

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 2013. Expenses were covered by the Federal Chancellery budget.
Staff	16 full-time and 8 part-time employees (21.85 full-time equivalent)
General Activity	
Decisions, opinions, recommendations	107 formal decisions (complaints), 326 Ombudsman cases and 49 authorizations (data transfer in third countries, research and surveys).
Notifications	11 404
Prior checks	4 193
Requests from data subjects	Writing: 1 136 Phone: no written documentation, up to 100 calls per day
Complaints from data subjects	Complaints leading to a formal decision: 107 Complaints leading to a clarification or recommendation: 326
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	160 million sector specific identifiers have been issued, over 10

² Federal Law Gazette (BGBl.) I No. 83/2013.

³Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

information	000 new persons, around 1.4 million new legal persons have been registered in the electronic identities register and 546 electronic mandates have been authenticated 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	16, 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. Data security of gas meters

In the reporting year, the Data Protection Commission made a **recommendation** to a gas supplier that it should take data security measures in respect of freely accessible **gas meters**, in order to **prevent access by unauthorised persons** to personal data stored in the gas meter.

The claimant had complained that, in the course of the new installation of gas pipes in the protected building where he lives, the gas meters were to be located in the corridor so that the meter reading, consumption (whether and how much) etc. would be accessible to an unlimited group of unknown persons (tenants and their families, delivery people, etc.).

The gas supplier countered that, for the location of the meter, technical security guidelines (General Distributor Network Conditions from the Austrian Association for Gas and Water, ÖVGW) and statutory requirements, as well as the space in the building, had to be taken into account. However, there was no “massive interference” in the claimant’s data protection rights, the existence of personal data was questionable, and the subject’s presence or absence in the apartment could not be inferred from the meter reading.

The Data Protection Commission found that **measures to guarantee data security** have to be taken for all organisational units of a client which use (personal) data. Depending on the type of data used and the scope and purpose, and with reference to the state of the technology and economic reasonableness (inter alia), it must be ensured that the data is not accessible to unauthorised persons.

If unauthorised persons – as a result of the generally accessible place of installation, as in this case – **are able to access personal data** which is covered by the fundamental right to data protection (Article 1 DSG 2000), **without any restriction**, this fundamental right of the data subject (the consumer) is violated.

2. Personal reference in statistics

In the reporting year, the Data Protection Commission made a **recommendation** to a health insurance fund, which was sending illness group statistics on the employees for a reporting year to interested companies with more than 50 employees on request, to tailor the statistics to each individual requesting company.

The statistical evaluations were structured such that various illness groups were listed in one column and next to them, in further columns, the sickness figures divided by men and women, as well as the resulting total number of employees affected, and the sick days, again separated by men and women, and the resulting total number of employees affected.

The purpose of transmitting the illness group statistics was to facilitate measures to promote occupational health.

The complainant was concerned that it might be possible for individual companies to make a direct connection between diagnosis and employees, so that the data provided was not indirectly personal or anonymised data in every case.

The Data Protection Commission agreed with these concerns and advised to the health insurance fund that a separation into male and female employees – and the associated breakdown of the illnesses typical for these groups (such as illnesses relating to the reproductive organs) – should only be applied if there are more than five people in one of these groups. The Data Protection Commission believes this number guarantees that it is not possible to identify specific employees.

If it is possible for an employer to identify a specific employee on the basis of the illness group statistics provided, the affected employee's right to secrecy with regard to his or her personal data according to Section 1(1) DSG 2000 is violated by the employer's inference. As health data is sensitive data within the meaning of Section 4 no 2 DSG 2000, a particularly strict standard has to be applied.

The Data Protection Commission thereby also confirmed the principle stated by the Constitutional Court that, even for basically non-personal statistics, it must also be ensured that their publication cannot lead to the identification of specific (worthy of protection and in fact safeguarded by the fundamental right to data protection) data (cf. VfSlg 12.228/1989). This principle is also reflected in Section 46(1) DSG 2000, which only provides for privileged use of data obtained for other investigations or other purposes if the intended scientific investigation or the statistics are not intended to produce findings on individuals.



BELGIUM

A. Summary of the activities and news

Amendments to the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (Privacy Law)

1. Suspension (subject to conditions) of the access right during an inspection or a tax investigation by the Ministry of Finance

Article 3 of the “Privacy Law” – which, for certain identified data processing operations, sets out special arrangements – since 2012 has provided for, amongst other derogations, suspension of the right to access to data related to processing managed by the Federal Public Finances Department during the period in which the data subject is the object of an inspection, an investigation or acts in preparation for these.

As this measure was deemed unacceptable by the Privacy Commission in particular⁴, this Article was amended in 2013. It is now laid down that the access right is indeed suspended in the aforementioned circumstances, *but only insofar as implementation of this access right would harm the requirements of the inspection, the investigation or the preparatory acts and only while these last*. The duration of these preparatory acts during which the access right does not apply *may not exceed one year from the access request*.

The exception is also immediately removed following closure of the inspection or investigation, or as soon as preparatory acts are closed where these do not lead to an inspection or an investigation. The security of information and protection of privacy department (internal inspection body) set up within the Federal Public Finances Department notifies the taxpayer in question immediately and communicates to them in full the *motivation* contained in the decision of the data controller that invoked the exception.

During this period when the access right is suspended under the conditions above, the data subject has an indirect access right – as in police matters – that he or she exercises through the Privacy Commission (Article 13 of the Privacy Law).

2. Creation of an inspection body for management of police information within the Data Protection authority (Law of 18 March 2014)

The Law of 18 March 2014 creates alongside the Privacy Commission a police information inspection body responsible for checking the handling of the information and data referred to by the Law relating to the functioning of the police. In the performance of its mission, this body is independent of the Privacy Commission, with which it does however share the Secretariat. Mainly made up of members of the federal and local police forces, as well as experts, the body must have an auditor from the inspection authority (Privacy Commission) amongst its members.

The inspection body is in particular responsible for checking compliance with the rules for direct access to the national police database (BNG) and for direct querying of this, and for checking compliance by all of the members of the police departments with the obligation to maintain this database. It ensures, through operational investigations, that the content of the BNG database and the procedure for processing the data and information stored in it follow the rules laid down by the Law on the functioning of the police and comply with their implementing measures, in particular the regularity of processing operations such as data entry and information being saved according to its concrete nature or reliability, and even the deletion and archiving of data and information at the end of their retention periods. Special

⁴ Privacy Commission, opinion 32/2012 of 17 October 2012 (<http://www.privacycommission.be>). In an order dated 25 March 2014, the Constitutional Court of Belgium, dealing with a request for cancellation of the initial amendment (before revision in 2013), cancels this provision.

databases (e.g. those with limited duration) are also inspected. The body has investigatory powers and reports as and when required and/or annually, to the Chamber of representatives.

Towards amendment of Articles 3 and 9 (right to information) of the Law "Private Life" Institut des Professionnels de l'Immobilier v Englebert et al brought before the Constitutional Court of Belgium and the Court of Justice of the European Union (CJEU)

The case aimed to find out whether Belgian law, by not providing any exemptions for private detectives similar to those referred to in Article 13(1) (d) and (g) of Directive 95/46, correctly transposes this provision. Indeed, by not providing any exemptions for private detectives, the duty to inform is applicable to them. The question was then raised as to whether, on the one hand, there was unfair treatment in relation to private detectives and, on the other hand, whether operating as a private detective was still possible under these conditions. In Belgium, the profession of private detective is governed by a Law dated 19/07/1991.

With an application made to it in 2012, in light of the questions that were raised, the Commercial Court asked the Constitutional Court of Belgium. The latter then contacted the CJEU.

The CJEU delivered its decision on 7 November 2013 (C-473/12): <http://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=182002>; the Constitutional Court of Belgium delivered its decision on 3 April 2014: <http://www.const-court.be/public/f/2014/2014-059f.pdf>

The Constitutional Court of Belgium deemed the provision in question of the Belgian "Privacy Law" of 8 December 1992 to breach Articles 10 (principle of equality) and 11 (principle of non-discrimination) of the Belgian constitution insofar as the duty to inform automatically applies to the activity of a private detective authorised to carry out their activities for public legal entities in accordance with Article 13 of the Law of 19 July 1991 "governing the profession of private detective" and acting for a public professional body (Institut des Professionnels de l'Immobilier) that is responsible by law for identifying breaches of ethics of a governed profession (real estate agents).

Amendment of the Law relating to electronic communications – new competence for the Privacy Commission on the subject of *data breaches*

Since April 2014, it is the Privacy Commission, and no longer the Belgian Institute for Telecommunications, that companies supplying electronic communication services to the public must notify in the event of data breaches. The Commission will in turn notify the Institute. The Commission is also obliged to ensure that these companies notify the breach to private individuals where this is required. A partnership is thereafter formed between the Belgian Institute for Telecommunications and the Privacy Commission.

Modification of the institutional data protection landscape

Alongside the *Vlaamse toezichtcommissie* (commission for control of the exchange of data between Flemish public services within the context of electronic administration), a commission for control of the exchange of data for the Walloon and Brussels regions was set up.

Activities of the Data Protection Authority

The annual report of the Privacy Commission gives details of all of its activities. Some of them merit particular attention (see <http://www.privacycommission.be>):

- **Education of minors:** the Belgian Privacy Commission initiated the staging of a funny, educational play on the subject of data protection (online activities and privacy) aimed at

primary school children (only in Dutch). It produced a complete educational kit, “Je suis jeune et je protège ma vie privée” (privacy protection for young people), one section of which is backed up by the aforementioned play. Visit the dedicated site <http://www.jeddecide.be> and <http://www.ikbeslis.be>

- **Data Breaches:** In the wake of several major data leaks (including the copying of the customer base file of the Belgian rail company concerning 1.4 million people), the Belgian Privacy Commission issued several recommendations intended to prevent such leaks, usually the result of inadequate securing of processed data.
- **Work on the draft EU Regulation (EU data protection reform):** the Privacy Commission delivered two important opinions within the context of data protection reform negotiated within the European Union. Its opinion 35/2012 relates to the proposed Regulation originally submitted by the European Commission, and its opinion 10/2014 relates to the text voted for by the LIBE Commission in October 2013.

Organisation	Privacy Commission
Chair and/or College	<p><u>1 January 2013 to 2 May 2013 inclusive</u></p> <p>Chairman: W. Debeuckelaere (magistrate)</p> <p>Vice-Chairman: S. Verschuere</p> <p>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 2012 Annual Report.</p> <p><u>2 May 2013 to 31 December 2013</u></p> <p>Chairman: W. Debeuckelaere (magistrate)</p> <p>Vice-Chairman: S. Verschuere</p> <p>College members: A. Junion (lawyer), F. Robben (general manager of the Banque Carrefour de la Sécurité Sociale and the e-health platform), J. Baret (honorary secretary-general of the Federal Public Justice Service), E. Gheur (managing director of Galaxia and lecturer at the university of Luxembourg), G. Vermeulen (professor of law at Ghent university), S. Waterbley (general advisor to the DG Telecommunications and information society of the Public Economy Service)</p> <p>College deputies: M. Salmon (advisor to the Court of Appeal in Brussels), S. Mertens de Wilmars (teacher), F. Schuermans (solicitor general at the Ghent Court of Appeal), Y. Roger (Chairman of the social security and healthcare sector committee)</p> <p>See also Article 24(4), paragraphs 3 and 4: “The Commission is formed in such a way that an equilibrium exists between the different socio-economic 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.”</p>

Budget	€6,840,000
Staff	<p>53 employees (1 Chairman – 1 Vice-Chairman)</p> <ul style="list-style-type: none"> - Chair'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), communications 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	<p>Opinions (upon request from the legislative or executive authority - see below): 69</p> <ul style="list-style-type: none"> - Opinions and initiative recommendations: 5 - Recommendations within the context of further processing declarations: 11
Notifications	6,047 declaration files in 2013 and a total of 5,252 new processing declarations. 436 declarations of amendments/corrections to existing data processing and 359 end-of-processing declarations
Prior checks	<p>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 received the following number of authorisation requests:</p> <ul style="list-style-type: none"> - Federal authority sector committee: 44 individual authorisations - Statistics sector committee: 28 individual authorisations - National Register sector committee: 87 individual authorisations - Social security and healthcare sector committee: consult the Banque Carrefour de la Sécurité Sociale website https://www.ksz-bcss.fgov.be/fr/bcss/nodepage/content/websites/belgium/security/committee_03.html
Requests from data subjects	<p>The statistics of the Belgian Privacy Commission do not make any distinction between requests for information from data subjects and those from data controllers:</p> <p>The Privacy Commission has processed 3,532 requests for information or mediation (including inspection files). These files can be broken down as follows: 2,871 requests for information both from public bodies and current or future data controllers and from data subjects, 450 requests for mediation and 211 inspection files.</p> <p>Its Front Office also processed 2,868 files on the following topics: use of surveillance cameras (14.85%), data protection principles (8.12%), work (5.47%),</p>

	economy (3.35%) (questions on consumer credit) and public authorities (2.24%).
Complaints from data subjects	<p>The Privacy Commission received 450 complaints, an increase of 48.5% compared to the number of complaints received in 2012 (303).</p> <p>These complaints are mainly in the following fields:</p> <ul style="list-style-type: none"> - Protection of privacy principles (27.6%): principle of proportionality, failure to respect the purpose principle, the duty to inform - Registration of delinquent clients with the Centrale des crédits aux particuliers (office for credits to private individuals) of the National Bank of Belgium (13.6%) - Videosurveillance (12.4%) - Direct marketing (5.1%) - Internet (4%)
Advice requested by parliament or government	The list of opinions issued by the Belgian Commission in 2013 is available on its website: 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	<p>211 inspection files.</p> <p>In 2013, the Privacy Commission carried out inspections at two 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 three 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.</p>
Sanction Activities	
Sanctions	The Privacy Commission 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 Privacy Commission 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 Privacy Commission does not have this information.

BULGARIA



A. Summary of the activities and news

Organisation	
Chair and/or College	<p>Under Art.7 (1) of the Law for Protection of Personal Data (LPPD), the Commission for Personal Data Protection is a collective authority consisting of a Chairman and 4 members.</p> <p>In 2013, the structure of the CPDP was: Mrs. Veneta Shopova- Chairperson and 4 members- Mr. Krassimir Dimitrov, Mr. Valentin Enev, Mrs. Mariya Mateva and Mr. Veselin Tselkov.</p>
Budget	BGN 2 700 000 of which BGN 2 693 530 are spent.
Staff	Number of employed officials: 67
General Activity	
Decisions, recommendations, opinions,	<p>In 2013, 357 decisions, opinions and instructions were issued in total, of which:</p> <ul style="list-style-type: none"> - 252 complaints - 79 opinions on the LPPD's application - 26 compulsory instructions
Notifications	42 308 personal data controllers
Prior checks	2 613 prior checks
Requests from data subjects	123 requests from individuals and legal entities and various inquiries on current issues of CPDP's competences.
Complaints from data subjects	<p>450 complaints — the most were received from the following sectors:</p> <ul style="list-style-type: none"> - Telecommunications- 333 - Labour and insurance services- 42 - Banks and Banking Services- 33 - Healthcare and Education- 13 - Others- 29
Advice requested by parliament or government	<p>In the reported period 2 requests for opinions were received from the Council of Ministers, as follows:</p> <ul style="list-style-type: none"> - Request for an opinion on two requests for access to public information- a media organization requested a list of employees under official and civil contract in the Council of

	<p>Minister's administration, containing names, positions, and remunerations under contract.</p> <p>- Request for an opinion on a question posed by two deputies via the Chairman of the National Assembly to the Prime Minister of the Republic of Bulgaria under Art.90 (1) of the Constitution of the Republic of Bulgaria and Art.89 of the Rules of Organization and Procedure of the National Assembly. They requested information on the number of employed and dismissed officials in the state administration for a 6 month period, specified by the body, as follows: Ministries, state agencies, executive agencies, local administrations, and specialized administrations - legal entities.</p>
Other relevant general activity information	<p>13 notifications and 12 requests for approval of third country data transfers were received. For the first time, a request based on binding corporate rules was submitted. Because this instrument was not foreseen by the Bulgarian legislation, in this case, the Commission approved the transfer on the ground of Art.36b of the LPPD, namely, on the basis of evidence submitted in regard to contractual obligations undertaken between the controller and the recipient providing sufficient guarantees for their protection.</p> <p>With regard to the established procedure by the Article 29 Working Party on Binding Corporate Rules, CPDP has approved lead authorities on 15 BCRs and agreed with the lead authority's decisions on 5 BCRs.</p>
Inspection Activities	
Inspections, investigations	<p>In 2013, a total of 2 696 inspections were conducted, as follows:</p> <ul style="list-style-type: none"> - ex-ante 2 613; - on-going 39; - <i>ex-post</i>: 44, mostly in the fields of: healthcare: 1 510; trade and services: 310; education and training: 225; legal and other consulting services: 136; construction and architecture: 62; tourism: 51.
Sanction Activities	
Sanctions	<p>In 2013, as part of its administrative-penal activities, the CPDP drafted:</p> <ul style="list-style-type: none"> - 30 findings of administrative violations - 29 penal decrees

Penalties	In 2013, the CPDP imposed fines and material sanctions in the amount of 76 800 BGN.
DPOs	
Figures on DPOs	N/A- the LPPD does not foresee the appointment of data protection officers.

B. Information on case-law

1. With regard to the issued compulsory instructions and penal decrees

In 2013, 26 compulsory instructions were issued, most of which were in the state administration sector, followed by local and municipal administration, finance, insurance, and health care. The fewest instructions were issued in the following sectors: justice, education and training, information technology, trade, and services.

The instructions were issued in connection with:

- the lack of necessary organizational and technical measures for ensuring the level of protection of personal data: 44 % of the decisions;
- the failure to take necessary action to update the information submitted in data controllers' registers: 18 %;
- unlawful processing of personal data: 25 %;
- processing personal data without the data subject's informed consent: 13 %.

In 2013, the CPDP issued 29 penal decrees (PDs). None of these were set aside by the court, and 1 was confirmed with a reduction of the fine. Of the decrees issued in 2011 and 2012, but appealed against and decided by the court in 2013, 3 were set aside in their entirety, 12 were confirmed, and 6 of these had the fine reduced. Currently, 25 PDs are still pending in court. In 2013, five PDs entered into force without having been appealed.

Among the most common violations of the LPPD were:

- violation of the principles of lawfulness, proportionality of the personal data processed, and processing for specific, precise, and legitimate purposes: 15 violations;
- processing without a statutory requirement for admissibility processing: 20 violations, for which material sanctions were imposed;
- failure to take technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss and unauthorized access, rectification or dissemination, and other illegal forms of processing: 19 violations, for which material sanctions were imposed;
- processing before the controller had submitted an application for registration with the Register of Data Controllers and Registers kept by them and maintained by the Commission: 3 violations for which material sanctions and fines were imposed;
- processing for direct marketing purposes without providing the individual with the possibility to object to the processing: 5 violations for which material sanctions were imposed;

- refusal to assist the Commission in the exercise of its supervisory powers : 4 violations for which material sanctions were imposed;
- failing to make a decision on applications for access to personal data: 2 violations;
- failure to declare CCTV Register : 4 violations.

2. With regard to the issuing of opinions on requests and signals

Aside from the requests to CPDP received from state authorities, stated in the table above, the following opinions are of interest:

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

In 2013, various opinion requests were also submitted regarding access to the National Population Database maintained by Directorate General "Civil Registration and Administrative Services" (DG CRAS) at the Ministry of Regional Development and Public Works (MRDPW) or the civil status registers.

The personal data controllers continued to request direct access to the National Population Database which was motivated by the presence of legal interest or because of their activities and the exercising of obligations set in law (e.g. credit institutions request access in connection with clients' identification requirements stemming from the provisions of the Law on the Measures against Money Laundering).

The CPDP's practice on the requests for direct access to the National Population Database is that a distinction should be made between the submission of information (data) from the NPD by proven legal interest and the provision of direct access to the NPD.

The Commission has issued an opinion that no legal obstacle exists for the MRDPW - DG CRAS to submit particular information, i.e. personal data (not direct access) to the parties which requested them when they prove their legal interest according to the established procedures.

2.2. Requests for access to public information

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

Despite that, in 2013, the CPDP also pronounced on requests for opinions from state and local authorities related to the requests for access to public information.

2.2.1. Requests to the relevant state authorities (Council of Ministers) for submission of information about:

- names, positions, and remuneration for individuals under labour and official contracts, as well as copies of civil contracts. In this case, the CPDP was of the opinion that the required information in such volume falls under the "personal data" category because it can identify individuals and its processing is admissible only with individuals' consent.
- number of employed and dismissed officials from the state administration for a 6-month period, according to the status of the body, as follows: ministries; state agencies; executive agencies; local administrations, and specialized administrations. The Council of Ministers was required to provide a list with names as well as information about the grounds for employment. It was also pointed out that the submission of this information will identify particular administrative structures. In this case, the information could be provided (without the names of the individuals) in order to observe the legally set obligation of the controller.

2.2.2. Other requests for access to information

The Deputy to the Executive Forestry Agency to the Ministry of Agriculture and Forestry for the provision of information contains personal data on files related to the change of use and sale of land plots in forest areas. Before the requested information is provided, an account should be taken in regard to the legal requirements, the public interest both in relation to the questions raised by the Members of Parliament, and also in regard to the right to privacy and the existence of individuals' consent. The CPDP has expressed the opinion that the personal data controller can submit the files regarding information about sales and changes in the intended use of the land plots after the personal data in them is brought in a form that does not allow for the identification of the individuals, such as deletion or anonymisation by initials.

2.3. With regard to the requests connected to the prevention of conflict of interest by the occupation of high positions in the state administration

Another important issue, related with the access to information, containing personal data and handled by the CPDP in 2013, was the announcement of the declarations under the Law on Prevention and Disclosure of Conflict of Interests (LPDCI) on the official websites of the state institutions. In search of a balance between the public interest and the protection of personal data of specific individuals, the Commission accepted that the publishing of declarations should be done after explicit written consent of the affected individuals, in separate text to the same declaration. The Internet announcement of the LPDCI declarations without explicit consent of the individual would be a violation of LPPD. Thus, any declaration published on the official sites, without consent, should be removed until explicit consent is given. The announcement should not contain the signature of the declarer. In cases where the declaration contains other individuals' personal data, the consent of the affected individual doesn't reflect on them and they should be anonymised.

2.4. With regard to the access to sensitive data, contained in special registers

Other opinions of the CPDP in 2013 were connected with issues regarding access to so-called "sensitive data", for which processing is generally prohibited under Art.5 (1) of LPPD.

As an example may serve a case, a State Psychiatric Hospital in a Bulgarian town was approached by the Regional Directorate of the Ministry of Interior (Moi) with a request to provide an "updated list of the currently hospitalized mentally ill persons" in the hospital. In this case, the CPDP has expressed an opinion that the requirement for maintenance of a list of mentally ill persons by police and junior police inspectors laid down under Art. 20 (1) (7) of Instruction 13-2295 dated 2012 in the organization of operation at the Ministry of Interior on the territorial service to citizens, is contrary to the conditions for the provision of health information under Article 28 (1) of the Health Act, which protects the patients' rights, and in this particular case, the rights of the patients with mental disorders hospitalized in the respective State Psychiatric Hospital.

Furthermore, the Constitution of the Republic of Bulgaria contains several basic principles regarding mentally ill persons, namely, persons with physical and mental disorders are subject to special protection by the state and society (Art. 51 (3)) and the state shall protect the health of citizens (Art. 52 (3)). In addition, the text of the instruction is in absolute conflict with the provisions of Art. 157 (1) of the Ministry of Interior Act, which explicitly prohibits the collection of information about citizens in regard to their health conditions alone (Art. 157 (1) of the Ministry of Interior Act). In view of the aforementioned, the Commission expressed an opinion that the requested information (updated list of the hospitalized mentally ill persons under treatment) should not be provided. Such a provision would be contrary to the provisions of Art.4 (1) and Art. 5 (2) of the LPPD, the provision of Art. 28 of the Health Act, as well as the provision of Art. 157 (1) of the Ministry of Interior Act.

In this case, the provision of such requested information about the persons treated in this hospital would violate the principles of purpose limitation and proportionality, as laid out under Art. 2 (2) of LPPD.

2.5. Opinion on the members of Parliament elections

In 2013, the CPDP expressed an opinion on the request from the Chairman and the Secretary of the Central Election Commission on held members of Parliament elections.

First, the issue of whether it is necessary to register in the CPDP was raised in regard to the Initiative Committees for nomination of independent candidates for the National Assembly. The Commission has stated that the Initiative Committees for nomination of independent candidates under Art.96 (2) of the Election Code (EC) are personal data controllers and they have the obligation to register in the CPDP.

The second matter was connected with the members of Parliament elections, as well as with the amendments and supplements in the Election Code, adopted in February 2013, and according to which the Central Election Commission (CEC) has new obligations. In connection with one of them, to broadcast the CEC meetings live in Internet, the CPDP has expressed an opinion that this is lawful and admissible, considering the legally established obligation stemming from the new Election Code provisions and the performance of tasks in the public interest, i.e. in order to ensure the possibility for the public to be informed on important matters discussed during the CEC meetings.

2.6. The CPDP's opinion on the implementation in Bulgaria in the Foreign Account Tax Compliance Act of U.S. taxpayers

A question of substantial financial interest on which the Commission has expressed an opinion is the implementation in Bulgaria in the Foreign Account Tax Compliance Act of U.S. taxpayers, adopted by the U.S. Congress – FATCA.

The request was filed by the representatives of a bank based in Bulgaria, which was part of a multinational company. The main purpose of FATCA is to enable the U.S. tax authorities to combat cross-border fraud by U.S. persons with accounts and financial assets abroad. This objective will be achieved by building a global system for automatic information exchange which imposes an obligation on all foreign financial institutions to provide information to the American Internal Revenue Service (IRS) about all accounts of U.S. taxpayers or foreign companies that are owned by U.S. taxpayers. Thus, FATCA creates numerous new obligations for all foreign financial institutions. After a thorough analysis, the CPDP assumed that due to the fact that the Bulgarian bank has no current regulatory obligation to provide the personal data of its customers– individuals subject to the U.S. tax law to another data controller in the United States relating to the implementation of FATCA, there is no legal basis for the CPDP to allow data transfer to the United States. Data transfer based solely on the consent of the individuals would be excessive and contrary to the principle of the legality of the processing of personal data because of the lack of regulatory basis to require the consent of the individuals.

C. Other important information

In the reported period, the Commission for Personal Data Protection adopted a new Ordinance on the minimal level of technical and organization measures and the admissible type of personal data protection

On 30 January 2013, the Commission for Personal Data Protection adopted a new Ordinance on the minimal level of technical and organizational measures and on the admissible type of personal data protection. The Ordinance was issued on the grounds of Art.23 (5) of the Law for Protection of Personal

Data. It was published in the State Gazette on 12 February 2013. This Ordinance repeals Ordinance № 1 from 7 February 2007.

The Ordinance aims to ensure adequate personal data protection level depending on the data nature and the number of affected individuals when a violation occurs. The main personal data protection purposes are defined as confidentiality, integrity, and availability. Five personal data protection levels are introduced: physical protection, personnel protection, documentary protection, protection of the automated information systems, and/or networks and cryptographic protection. In addition, the Ordinance introduces the “need to know” principal.

In order to determine the adequate level of technical and organizational measures and the admissible type of protection, the controllers are obliged to perform periodic impact assessments on the processed personal data.

The impact assessment aims to define the levels of impact and the relevant protection levels. For every protection level the necessary technical and organizational measures which need to be undertaken by the personal data controllers are determined.

The new rules foresee four impact levels depending on the extent of the negative consequences on the individuals as a result of unauthorized personal data processing: “extremely high”, “high”, “medium”, and “low”.

Since the Ordinance was entered into force, the Commission for Personal Data Protection has started consultations and begun training personal data controllers to raise awareness of the new protection rules.

The Ordinance (<https://www.cdpd.bg/en/index.php?p=element&aid=632>) is available in English on the CPDP’s site.

The Commission for Personal Data Protection is focused on its current activity to train personal data controllers by following the adopted Annual Training Plan. The CPDP’s experts participate as lecturers on personal data protection issues in the courses of the Public Administration Institute, which is the only national training center for state administration officials.

CROATIA



A. Summary of activities and news

Organisation	
Chair and/or College	Anto Rajkovača
Budget	5 482 847 HRK (1€ - 7,5 HRK)
Staff	28
General Activity	
Decisions, opinions, recommendations	1 091
Notifications	21 978 (1 648 in 2013)
Prior checks	
Requests from data subjects	The requests are not separately registered
Complaints from data subjects	212
Advice requested by parliament or government	17
Other relevant general activity information	The Agency has adopted a new organisational structure which is focused on increasing inspection activities.
Inspection Activities	
Inspections, investigations	330
Sanction Activities	
Sanctions	87
Penalties	2
DPOs	
Figures on DPOs	2 037 registered DPOs (643 in 2013)

In the reported period, the Croatian DPA has been firmly dedicated to campaigns aimed at raising public awareness related to the importance of personal data protection. Consequently, we will inform you about the most important activities which have been realized over that period of time:

- The public introduction of the Ministry of Interior's "Red Button" online application for reporting the sexual abuse or exploitation of children under cooperation with the partnership in establishing a functioning "Centre for Safer Internet" (where Croatian Personal Data Protection

Agency is one of the strategic partners) all with the objective of raising public awareness regarding the safe use of the Internet and promoting the safe, responsible, adequate, and efficient use of the Internet by children and youth;

- On Data Protection Day 2014, the Agency organized a gala press conference with various activities such as the appointment of new Ambassadors of privacy (well-known persons who, despite their popularity, enjoy a very positive public reputation) with a mission to promote the privacy and protection of personal data;
- On its 10th anniversary the Agency organized a series of activities (in May 2014) which received a very good reception by the Croatian public, and these activities are as follows:
 - 1) **Gala press conference '10 steps against hate speech on the Internet'** held in the Croatian Parliament in the presence of many significant persons from the Croatian political and cultural life, including the Ambassadors of privacy who read very dramatic testimonies written by two Croatian adolescents who experienced very serious traumas due to the very ferocious forms of cyberbullying to which they were exposed during the very delicate period of life which is adolescence. In this way, a very important message has been sent to the public regarding the consequences of hate speech. A detailed report from this conference was broadcast in prime time by NOVA TV in its central informational program, which in Croatia has the highest ratings. Also, the representatives from the Ministry of Interior, Academic Research Network (CARNET), and Croatian journalists' association held presentations about the matter from their point of view.
 - 2) The Agency is very proud of producing **promo materials** with educational messages regarding the subject of hate speech on the internet which are as follows:
 - educational poster "10 steps against hate speech on the Internet" ;
 - roll-up poster 1: "Let's surf on the positive waves!";
 - roll-up poster 2: "Everyone has the responsibility!".
 - 3) **The Conference for data protection officers and information officers** with 5 eminent guest lecturers (experts) who held very informative presentations covering the latest trends in data protection and neighbouring fields. The Agency was highly praised for the initiative of organizing such a conference which provided much useful information to more than 100 participants.

CYPRUS



A. Summary of activities and news

The Commissioner's Office was consulted on a number of EU legislative proposals, inter alia, the data protection Package of Proposals presented by the Commission in January 2012 and the proposals regulating Europol and Eurojust, in issues relating to the protection of personal data.

The Commissioner's Office was actively involved in the Council of Europe's works for the modernization of Convention 108 for the protection of individuals with regard to automatic processing of personal data, participating at the CoE's relevant T-PD and CAHDATA Committees.

In the framework of activities for celebrating European Data Protection Day, the Commissioner's Office allocated a budget of €4,300 for disseminating, on January 28, printed information material and gifts (alarm clocks and light torches) with the Office's logo and email 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.

Pursuant to the examination of a complaint filed by employees, through their Unions, against a private hospital that had installed a biometric system for monitoring work attendance, making use of (fingerprints) stored in smart cards issued to employees, not stored in a central database, a Decision was issued concluding that the use of these systems, for this purpose, was in breach of the proportionality principle. The hospital was called to cease processing and uninstall the system. The hospital did not comply 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: €257 352 Executed budget: €225 120
Staff	Administrative Officers: 7 Information Technology Officers: 2 Secretarial officers: 6 Auxiliary staff: 2
General Activity	
Decisions, recommendations, opinions,	Opinions: 61 Decisions: 5 Recommendations: 2
Notifications	278
Prior checks	N/A
Requests from data subjects	In writing or by phone: N/A
Complaints from data subjects	Spam: 308 Other: 77
Advice requested by parliament or government	On 21 occasions our Office was invited to Parliamentary Committees of the House of Representatives for advice/consultations
Other relevant general activity	Licenses for combination of filing systems: 16

information	Licenses for transmissions to third countries: 50
Inspection Activities	
Inspections, investigations	Number of Audits: 1
Sanction Activities	
Sanctions	In 3 out of 5 Decisions, Administrative Sanctions were imposed. In the other 2 Decisions, the Commissioner issued Recommendations to controllers.
Penalties	In 2 out of the 3 Decisions where Administrative Sanctions had been imposed, controllers were fined €3 000 and €300, respectively.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

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 conditions and the number of (additional) documents that the complainant had at times been requested to submit, in 2013, the Commissioner issued a Decision concluding that the insurance company failing to either accept or reject the claim within a reasonable amount of time, while taking into account a proportional number of documents that the complainant had been asked to submit at times and prolonging the examination of the claim by asking for additional tests and documents, constitutes an infringement of the proportionality principle and imposed an administrative sanction of €3 000 on the company. The Commissioner's Decision was challenged before the Court and the ruling is pending.

C. Other important information

The Council's 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 was transposed into national legislation on 20 December 2013, by virtue of a relevant Decision issued by the Council of Ministers. The national law appoints the Commissioner as the competent supervisory authority stipulated by the Decision.

CZECH REPUBLIC



A. Summary of activities and news

The supervisory activities centered on the Office's inspection plan as well as citizens' complaints. Selected cases are described below. Thus, the areas of planned supervisions, namely, were: DP processing in the national Schengen information system, processing of data regarding donation beneficiaries (e.g., ESF funds), handling of data by public administration bodies, processing of PD in the sector of services, and commerce.

On 11–12 February 2013, we hosted a **study visit** from the Moldovan DPA. The event was funded and logistically backed by TAIEX. Topic: Protection of Personal Data in Written, Visual, and Audio-visual Media.

On 21–22 May 2013, we hosted a TAIEX-funded **study visit** from the FYROM DPA. The event was funded and logistically backed by TAIEX. Topic: Data protection in the Schengen information system.

Moreover, two of our experts took part as speakers in TAIEX workshops in Moldova, Bosnia, and Herzegovina, respectively.

On 15–16 April 2013, we hosted the **53rd meeting** of the International Working Group on Data Protection in Telecommunications (**IWGDPT**) in Prague. Two documents were adopted there:

- Working paper on web tracking and privacy: respect for context, transparency, and control remains essential
- Working paper and recommendations on the publication of personal data on the web, website context indexing and the protection of privacy.

Implementation of the **Leonardo da Vinci Partnership project** focused on 'Raising awareness of the data protection issues among the employees working in the EU' has been ongoing. The aim is to offer a comprehensive handbook reaching out to a broad audience of European employees and to organize side events to raise public awareness. Project partners are DPAs from Poland (project coordinator), CZ, Bulgaria, and Croatia. The project end is set for July 2014.

Organisation	Office for Personal Data Protection
Chair and/or College	Mr Igor Němec (President of the Office)
Budget	CZK 128 731 000 (EUR 4 694 785, exchange ratio 1 EUR = 27,42 CZK)
Staff	100
General Activity	
Decisions, opinions, recommendations	6 opinions (most of them concerned more or less with the monitoring of citizens) 1 comprehensive recommendation – methodology for e-shop operators
Notifications	6 570 notifications (out of which 5 994 registered, with 576 still ongoing or suspended)

Prior checks	85
Requests from data subjects	2 994 (out of which 15 were from abroad)
Complaints from data subjects	1 336 (plus another 7 428 concerning spam)
Advice requested by parliament or government	No such activities in 2013
Other relevant general activity information	79 requests pursuant to the Free Access to Information Act. 69 bills and 95 implementing regulations commented on within inter-ministerial comments procedure International transfers authorization: 25 requests of which 20 were permitted, 1 was declined, 4 were suspended due to procedural reasons
Inspection Activities	
Inspections, investigations	90 (out of which 74 were accomplished) + 91 investigations concerning spam (all accomplished)
Sanction Activities	
Sanctions	ca. 61 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 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	ca. 155 penalties
DPOs	
Figures on DPOs	Not applicable in the Czech Republic.

B. Information on case-law

Based on several complaints, we conducted an **investigation of three ski-lift operators** in three different winter resorts. All skiers were photographed and measured by a laser chip upon buying their ticket or ski-pass (the complaints were primarily concerned with the season ski-passes). The photographs, together with the name and surname, body height, and ticket number, were stored in a database. The stated purpose was prevention of misuse of these ski-passes (they were often used by more than one person). The skiers were, upon check-in at the lift, controlled – their data matched the presented ticket. The data were deleted after the season had finished. The investigations revealed that all operators (they all were data controllers at the same time) breached the law in two instances: 1. Failure to provide data subjects with information about the respective data processing, 2. Failure to notify the processing operation and get registered with the Czech DPA. Therefore, we imposed non-financial sanctions on all three operators (they were obliged to take appropriate remedial measures).

We conducted an inspection of the Czech side of **EURODAC**. The inspector randomly choose a number of records, checked the on-site procedures (there are three sites in the Czech Republic where fingerprints and other relevant data are captured and stored). The inspection has not revealed any breach of the

data protection law. However, the Czech Interior Ministry welcomed our recommendation concerning the need for better feedback communication between the EURODAC operator and the register offices (e.g. information in case the asylum seeker obtained citizenship through marriage).

Initiated by numerous complaints (concerned namely with the disclosure of untrue or incomplete data and failure to delete unlawful data upon request) we conducted **an inspection at the Central Registry of Debtors (CERD)**. It was discovered that the investigated entity is only a processor whilst the controller is established in the USA. The inspection revealed a breach of the data protection law in two instances: 1. Failure to collect personal data only for the declared purpose and to the extent adequate for this purpose, 2. Failure to respect the data subject's rights in cases regarding the unlawful processing of data. We imposed remedial measures on the processor and obliged them to inform us about their fulfilment. Also, we recommended improving the understandability of the offered services to prevent further complaints.

We conducted an investigation into the security of data processed in the unified **information system of work and social affairs** whose controller is the Czech Ministry of Work and Social Affairs. We discovered that the system enabled usage by multiple officers via one common username and password. It was operated without logging in, as well. Therefore, we ordered them to take two remedial measures: 1. to provide all authorized officers with their own username and password, 2. to ensure that access logging is introduced by the software supplier.

C. Other important information

Our supervisory staff conducted several inspections at three Czech embassies, sometimes in the margin of a business trip to a conference or other event.

In 2013, we started an inspection in relation to the migration from SIS 1+ to SIS II. The purpose was to check how the Police of the Czech Republic, as controllers of data processing in this system, have been providing protection for personal data. The inspection has been focused on procedures as well as on the technical and physical security of data. This inspection is still ongoing in 2014.

Awareness raising – our experts conducted 33 lectures on data protection law at public institutions and local administration bodies as well as private entities.

In 2013, we prepared for the launch of the office's new website. It was adapted in visibility and its functionalities enhanced whilst the structure remained so as not to confuse regular users.

DENMARK



A. Summary of activities and news

Organisation	
Chair and/or College	The day-to-day business of the DPA is attended to by the Secretariat, headed by a Director. Cases of a principle interest (approx. 15 cases per year) are put before the Council for a decision. The Council is chaired by a Supreme Court Judge.
Budget	Approx. 22.5 million DKK
Staff	Approx. 35
General Activity	
Decisions, opinions, recommendations	N/A (included in the figures below)
Notifications	2 777
Prior checks	2 777
Requests from data subjects	2 221 This number covers all requests and complaints made to the Danish DPA
Complaints from data subjects	See above
Advice requested by parliament or government	468
Other relevant general activity information	14 cases relating to security
Inspection Activities	
Inspections, investigations	45
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	N/A
DPOs	
Figures on DPOs	N/A (this is not an option according to the Danish legislation)

B. Information on case-law

Public institutions using social media sites

In October 2013, the Danish Data Protection Agency (DPA) received an inquiry from a public institution regarding its use of social media sites – particularly Twitter and Facebook. The institution was planning a pilot project in which it would be more publicly present on social media sites.

In this situation, the Danish DPA have two main points. First, the authority should manage their postings on social media sites in a way that does not include personal data. Natural persons are – as a main rule – the data controller for their own postings on social media sites.

Second, if it will be possible for citizens to contact the authorities through the internal mailing systems on social media site, then those authorities can become the data controllers of that data, just as it is possible to consider the social media sites to be data processors. Therefore, the authorities must take the management of the internal mailing system into consideration.

If the authorities are to be considered data controllers, and the social media sites to be data processors, then said authorities will have a responsibility regarding data security, and might have to make a data processing agreement with the social media sites, just as the authorities have to consider the regulations regarding the transfer of data to third countries.

Personal data in demerging companies

In March 2013, the Danish DPA received an inquiry from a law firm concerning a situation where a company will demerge into more independent companies through re-structuring. The question regarded, in particular, is if the company will be considered to be in succession, or if it should be considered as the transfer of the personal data of the customers and clients to another company.

The Danish DPA found that it – as a main rule – will be considered as a transfer of data, as data will be passed from one company to another. But, in some cases, it will be possible to consider it as a succession of the company.

In those situations, the following elements must be observed: The relation to the costumer/client (rights and obligation) is transferred, the transferred assets will continually be in operation, the succeeded division of the company is strictly defined, the company can stand alone, and the sole purpose of the transfer is restructuring.

If the above situation is the case, then it can be considered as a succession in regards to the personal data. It is up to the data controller to make the preliminary assessment.

C. Other important information

Video surveillance in taxis

Since 2010, it has been a legal requirement for Danish taxi companies to equip taxis with video surveillance. Therefore, the Danish DPA conducted a series of inspections of taxi companies with the purpose of confirming whether the video-installation complied with data protection regulations, and to gather information on how the data controllers are handling video surveillance.

The DPA found that, all in all, the taxi companies had a sufficient understanding of the data protection requirements, as there were no major discoveries in the inspections.

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 great knowledge and interest in personal data protection.

ESTONIA



A: Summary of the activity and news

The development of information and communications technology and the information society is rapid. Thus, there is an extensive “grey” area in the acquisition of personal data protection and public information.

Undefined legal concepts (e.g. excessive damage, public interest) therefore require constant interpretation. Considering how small the Estonian law and language space is, our specialized legal scientific commentary and judicial practice takes more time to develop than that of bigger countries.

Therefore, the Inspectorate must focus more on creating guidelines, and developing legal practices, in order to ensure legal clarity and legal certainty essential in public administration and business.

Each year, the Inspectorate has undertaken some significant “gray” area subject, organized monitoring, investigations, and discussions involving relevant parties and eventually taken the professional idea and practical problems as a guideline.

*

Last year, this central topic was the use of monitoring and recording equipment. We tried to approach this in a complex manner: use of cameras for private purposes, recording in a public place and at a public event, security cameras, recording to ensure contract enforcement and for journalistic purposes, cameras in children’s, educational, and public institutions, etc. One of the issues causing debate, for example, was whether the kindergarten and school are public places from the point of view of recording and photographing (where consent is not necessary) and if they are, to what extent.

The Inspectorate’s Legal Adviser, Maris Juha, initiated the preparation of “Camera use guidelines”, which was our first guideline to be published in the draft legislation information system.

*

In addition to preparing new guidelines, we also try to keep our other important guidelines “alive”, refer to them in our daily work, and monitor the need for change. It turned out that, in addition to the guideline about personal data processing in employment relations, which was prepared in 2011, a need arose to more thoroughly cover the privacy of employees’ use of computers and smart devices.

While in personal relations it is covered by an individual’s confidentiality of messages and a communications company’s data protection and secrecy obligation, the use of the same devices in employment relations creates a legal triangle – an employee is not the customer of a communications company. The guideline “Employee computer use privacy” initiated by the Inspectorate’s IT-adviser Urmo Parm binds together both information technology and legal explanations.

In addition to publishing the answers to questions that are of most interest to employees and employers in our website’s frequently asked questions section, we will also publish them in the working life portal managed by the Labour Inspectorate.

*

Last year, there were several issues in the area of insurance – use of third-party data, storage of personal data processing consents, and customer data movement with a broker changing employers. On the initiative of Leading Inspector Merit Valgjärv, we also carried out monitoring of leasing companies in connection with the transmission of personal data to insurance companies.

In banking, we performed contract-based and consent-based examinations of the processing of personal data and also organized monitoring to acquire an overview of the practices. The main problems occurred in connection with direct marketing consents. The banks have now adjusted their practices in this area.

Based on problems revealed in practice, we made extensive improvements in the payment defaults publication guideline.

*

Formation of the Inspectorate's IT-group has significantly improved explanation and awareness raising activities in the area of information and communications technology. We will publish practical explanations and instructions in the press and on the web. Nine practical recommendations for the safe use of a smart phone by IT-adviser Urmo Parm gathered more than 21 thousand views on the Inspectorate's Facebook wall. Instructions for Facebook applications were viewed more than 10 thousand times. For the setup of browser vendors of a child's computer (directed towards parents), they were viewed almost 10 thousand times, and for deleting ID card user history on a computer, 4 thousand times.

We also performed awareness raising activities through various forms of cooperation – in the project Targalt Internetis (Be Smart Online), with the Association of History and Social Studies Teachers and web constables. On the initiative of Adviser Silver Sarapuu, we prepared comic books related to the protection of privacy to be used as auxiliary materials by teachers at schools.

*

In cooperation with Tartu University, we organized the conference “Ethical Dimensions of Data Protection and Privacy. Global and Local Challenges” on 9-10 January, 2013. The selection of speakers was impressive, including several top scientists from Estonia and internationally renowned foreign lecturers, such as Prof. Beate Rössler and European Data Protection Supervisor Peter Hustinx. The patron of the conference was the President of the Republic, who also held the first presentation on the topic. A financial sector Explanation and awareness raising activities Conference was held in cooperation with the University of Tartu Centre for Ethics

For such a high-level and, at the same time, comprehensive research event, we must first and foremost thank the head of the University of Tartu Centre for Ethics Prof. Margit Sutrop and her team. The conference audience mainly came from a legal or information technological background and I believe both were impressed by the conceptualization of their daily work through ethical values.

*

Approval of databases in the state's information system management system is a procedure between agencies, which is dry and dull on the outside and in which the public is not particularly interested. An exception turned out to be the approval of the public transport ticket sales information system in Tallinn.

Since the local government ignored legal and information security-related remarks by the Inspectorate and the State Information System Authority and made use of an uncoordinated database, we initiated separate supervision proceedings, in which we involved experts from both the stated Authority and the Centre of Registers and Information Systems. As a result, personalized data storage periods were shortened, security was strengthened, relevant local government legislation was amended, and the database was subjected to concertation proceedings.

All the changes made as a result of supervision would have come out in due course during the approval of the database establishment plan stage or the approval of implementation stage at the latest.

We believe this is a lesson for all state and local government agencies – solving data protection problems in databases retrospectively is more expensive and cumbersome than screening them out during the course of approval.

We compiled “Database guidelines” to solve practical issues related to the regulation and management of databases.

*

In cross-border activities, we continued the cooperation between data protection inspectorates of the Baltic countries and supervision carried out using a common methodology on agreed topics.

We completed the tripartite monitoring of the hotels using the trademark Radisson Blue Hotel. In monitoring casinos, we discovered a loophole in Estonian legislation regarding the maximum period for storage of video recordings and customer information for the correction of which we gave a recommendation in cooperation with law enforcement authorities and the union of organizers of gambling.

Data protection agencies in the Global Privacy Enforcement Network (GPEN) carried out Internet Sweep Day monitoring in May 2013. Within that framework, we examined the existence and comprehensibility of privacy policy in 40 of the largest retail companies in Estonia.

According to the Directive, the purpose of the activity of the European data protection authorities' working party formed on the basis of article 29 of Directive 95/46/EC is to improve the harmonized implementation of the Directive. To date, the working party's most voluminous activity has overwhelmingly been the preparation of opinions (guidelines), in which we have achieved a considerable proficiency. Policy advice is also dealt with – recently, and in particular, with the EU data protection rights reform in coordinating the solving of cases that have attracted international attention and, if necessary, some member authority is given the right to act on behalf of the entire working party.

In October 2013, the Inspectorate presented an initiative at the working party's plenary session to regularly enter on the agenda some organization of practical cooperation – an exchange of managerial experiences and an agreement on smoother cross-border cooperation procedures. The initiative was supported and was joined by colleagues from the United Kingdom. In all subsequent plenary sessions, all jointly prepared agenda items have been discussed.

*

In responding to breaches, the Inspectorate's priority is still the quickest possible termination of the breach as opposed to punishment.

This approach is also supported by the study “Access to data protection remedies in EU member states” published by the European Union Agency for Fundamental Rights in January 2014 – data subjects, whose rights have been violated, are primarily interested in the quick termination of the violation.

According to the Inspectorate, disputes related to the availability of public information serve the same purpose – persons making requests are interested in quick and easy proceedings to gain access to information.

For comparison – in supervision cases related to the protection of personal data and public information, 287 proposals-recommendations and only 53 precepts were made. In the majority of cases, the violation ends with receiving a proposal or a recommendation.

The punitive response (misdemeanour proceedings) volume has decreased and it mainly includes misuse of professional access rights to sensitive records. Since the violation has already taken place, supervision

by making proposals-precepts is no longer relevant, which is why the Inspectorate always responds by initiating misdemeanour proceedings in these cases.

The situation with the population registry has significantly improved. We acknowledge years of systematic usage monitoring by the Ministry of the Interior responsible for the registry. It was probably also helpful that the Inspectorate covered this topic in the media.

In the course of the Road Administration’s data protection audit, we examined the vulnerability of personal data in the undisclosed part of the traffic register – this includes the contact information based on the population register. Today, the Road Administration has implemented technical measures and internal control to prevent misuse and, based on an agreement entered into last year, notifies the Inspectorate of suspected breaches to initiate a misdemeanour case.

Organisation	Estonian Data Protection Inspectorate
Chair and/or College	Director General
Budget	631 329 €
Staff	18
General Activity	
Decisions, opinions, recommendations	601
Notifications	602 registrations of processing of sensitive personal data
Prior checks	15
Requests from data subjects	1 370
Complaints from data subjects	550
Advice requested by parliament or government	52
Other relevant general activity information – approval of public sector databases (including refusals)	89
Inspection Activities	
Inspections, investigations	463
Sanction Activities	
Sanctions	22 cases
Penalties	3 206 €
DPOs	
Figures on DPOs	121

FINLAND



A. Summary of activity and news

As part of the implementation of the strategy of the Office of the Data Protection Ombudsman during the year under review, we restructured our personnel planning system and integrated our internal competence management programme more thoroughly into the system. To ensure continued success in a volatile operating environment, we must secure the quality and quantity of internal competencies. Other cornerstones of our strategy include the ability to predict the impact of new phenomena and to prioritise our measures, the utilisation of information as a steering tool, and the formation of necessary alliances while retaining our independence and impartiality.

The Office also succeeded in achieving the level required by the Government decree on information security. As part of the effort, the entire personnel was obligated to take an information security test. Information security training is a permanent part of our competence management programme.

We initiated measures to launch an entirely new service function, information services, and to restructure our personnel. Development of internal information management forms a part of this path. I believe that the greater part of issues raised with us have already been commented or acted upon by us earlier. Efficient management of resources and continued maintenance of the service level requires us to focus on essential issues.

Independent of the completion of the data protection regulation or directive, we are aware that there is a dire need, in regard to competence in our country, to be able to fill the increasing number of positions opening up for Privacy Officers. Therefore, we launched an internal survey to investigate the potential of creating a brand for the required training. This product development effort is to be carried out in cooperation with educational organisations in accordance with our strategy.

As part of striving towards maximum effectiveness, we continued our business sector- and phenomenon-specific surveys. These surveys concerned targets such as telephone services financed through advertising, the payday loan industry, commercial use of personal data, and website information security surveyed in international cooperation (Sweep Day).

Consistency mechanisms and international cooperation were practiced in cooperation with our Norwegian colleagues by launching a joint audit of a global online music services conglomerate. The audit was completed during the current year.

Our areas of emphasis included data protection for entrepreneurs. Entrepreneurs have been targeted by a variety of forced selling operations. To ensure their legal protection, the proper balance of information between the parties in dispute is important. Within our sphere of competence, we supported the Federation of Finnish Enterprises in conquering the problem.

Biobanks were introduced as a new target group among the Data Protection Ombudsman's personal data protection duties. The National Supervisory Authority for Welfare and Health (Valvira) will act as the primary supervising authority.

Organisation	
Chair and/or College	Reijo Aarnio has been the Data Protection Ombudsman since the 1st of November 1997.
Budget	The overall annual budget is € 1 708 000.
Staff	The total number of staff is 20.

General Activity	
Decisions, opinions, recommendations	3 157
Notifications	535
Prior checks	see notifications
Requests from data subjects	958
Complaints from data subjects	(access and rectifications) 269
Advice requested by parliament or government	127
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	119
Sanction Activities	233
Sanctions	N/A
Penalties	N/A
DPOs	
Figures on DPOs	>1000

B. Information on case-law

Police cases

It became publically known that personal data of the President of Russia had been recorded into the information system of the Finnish police. At the same time, investigations were in progress concerning the unauthorised viewing of the data of a deceased Olympic gold medallist. The investigation led to dozens of employees of the police being found guilty of a violation of the provisions of personal data file legislation. The situation threatened to affect public trust in the police and the position of the commanding officers of the Finnish police. My personal view is that the chain of command within the police from the top to the officers who process information is too long and requires the inclusion of supervision carried out closer to the actual operations.

Food safety

Frequent shopper systems have traditionally gathered information on the consumers' shopping habits at a general level with the consumers' permission. Product-specific information has not been gathered. The Finnish Food Safety Authority Evira was informed of the possibility that a product sold by a retail chain

with a frequent shopper system had contained toxic *Datura stramonium*, leading to consumers having to seek medical treatment at hospitals. Based on Article 19 of the general European food regulation (Regulation (EC), No 178/2002 of the European Parliament, and of the Council), Evira required that the retail operator takes measures to connect the frequent shopper system's information to the shop's purchase data in order to warn the consumers who had purchased the product in question. It was revealed that the shop was indeed able to connect these data. This resulted in lively discussion concerning the credibility of frequent shopper systems and, on the other hand, the relationship between data protection and product safety.

Affiliate marketing

The Act on the Protection of Privacy in Electronic Communications states that prior consent is required for electronic direct marketing targeted at consumers. To circumvent this unambiguous rule, affiliate marketing has been developed. In affiliate marketing, the actual marketing measure is taken by a company operating in an opt-out country, for example. The company that wishes to sell its products purchases marketing services from the other company, but claims not to purchase personal data processing services or personal data content. In one type of affiliate marketing operation, publishing space is purchased from another company's marketing communication materials or other communication materials. The Data Protection Ombudsman intervened in these operations. Codes of conduct concerning such marketing actions are now being prepared together with the direct marketing industry.

Definition of a controller for a personal data file

It has come to my attention that the representatives of a religious group have visited homes and collected personal data, neglecting to observe the obligations set out in the Personal Data Act. The issue was not whether the denomination is allowed to gather data as part of its operations, but who was responsible for the data collection operations as the controller. The denomination denied its responsibility and explained that the case concerned use of personal data for domestic purposes for which the Personal Data Act does not apply. My view of the matter differed from this, and the Data Protection Board, which acted as competent authority in the matter, shared my view. The denomination appealed against the decision at an administrative court.

C. Other important information

The new ecosystem of mobile communications set an increasing challenge to data protection and the position and rights of consumers on a more general level. Smartphones have taken us to the age of apps, or applications. Processing of personal data is moving from traditional central register files to increasingly complicated systems where large numbers of applications are run over the operating systems of devices connected to a network infrastructure.

In this context, a national cyber security strategy was issued in Finland.

The Ministry of Transport and Communications carried out a survey of the current Big Data theme, and the Ministry of Finance appointed a working group to implement an open data programme. Operators continued to suffer from the deficient transfer of information between authorities. To remove the part of the problem that is due to the lack of an overall information system architecture, it was decided that a new authority that would employ more than a thousand people (Valtori) would be established as a corrective measure. Similarly, the citizens' service channel was developed, partly based on Estonian experience.

A legislative framework concerning the protection of personal data has been continuously developed. On the other hand, the process has increased our supervisory duties. The adequacy, or more appropriately, the scarcity of our resources seems to be a permanent condition, based on the survey carried out in connection with the NETSO project and pending publication.

The Information Society Code legislation project led by the Ministry of Transport and Communications proceeded swiftly. The project also raised the issue of net neutrality, or whether all Internet communications should continue to flow freely or whether the operators, for example, have the right to give priority to some messages, i.e. those that are paid for with higher rates.

The report by Professor Ahti Saarenpää discussed, in accordance with the assignment, the potential need of a positive credit record. The rapporteur reached the conclusion that it would be better to first observe the impact of the European data protection regulation on the processing of financial information. On the other hand, the rapporteur proposed that credit records should be identified as one of society's fundamental data files, resulting in special statutory privileges being allocated to them.

Emotions were also raised by the work of the road traffic taxation working group chaired by Mr Ollila. I was opposed to real-time tracking of drivers and proposed that when data is required for use as a basis for taxation, it should be collected in a distributed manner.

A survey carried out by us showed that nearly all telecommunication operators who offer mobile subscriptions to consumers also offer an option with partial financing through advertising. The consumer consents to receiving advertisements in exchange for a discount on call prices. According to consumer authorities, a telephone is a necessity. The Data Protection Directive defines consent as a one-sided, withdrawable legal act. Consumers frequently subscribed to a service partially financed through the reception of advertisements, and then immediately withdrew their consent. The Data Protection Ombudsman established that in the case of such necessary products, the consent cannot constitute part of the customer agreement, but must be considered a separate declaration of intent instead. As a result, operators developed a special double pricing system.

Communication of necessary information to the public constitutes one of the biggest challenges of data protection. To relay correct and well-timed information, a restructuring of our website was in process in 2013. We also participated in the development of the overall concept of the Tietosuoja magazine and made a decision to establish an information service group.

FRANCE



A. Summary of activity and news

2013 once again saw a significant increase in activity, demonstrating the predominant place of personal data in the digital age and an increasing sensitivity amongst citizens on this subject. Faced with this growth, the CNIL (*Commission nationale de l'informatique et des libertés* - the French data protection authority) has continued to take action and has adapted to become even more responsive.

The development of compliance tools

Throughout 2013, the CNIL continued its approach to support professionals by offering them various tools to assist with compliance, such as “Data Protection” correspondents, labels, internal company rules (BCR) and the creation of sector compliance packs.

“Data Protection” correspondents involved in co-regulation

Each year, Data Protection contacts assert themselves as key players in compliance.

At the end of 2013, 13,000 bodies had appointed a Data Protection contact, compared with 11,000 one year earlier. The added value of appointing a Data Protection correspondent becomes particularly significant in new projects involving the processing of personal data, because of the advice given, when handling a complaint or a CNIL inspection, and lastly in facilitating the exercise of rights of access and opposition.

Called upon to take over from the Data Protection contact with enhanced missions, the future data protection officer will be at the heart of the model proposed by the draft European Regulation.

Labels: instilling confidence

The Data Protection Act enables the CNIL to issue labels “to products or procedures”. The CNIL label means that companies stand out in terms of quality of service. For users, it instills confidence in the labelled products or procedures, by enabling them to easily identify and choose those that guarantee a high level of protection of their personal data.

Three reference systems have been created at the request of professional organisations: the “training” label and the “processing audit” label, adopted in 2012, and the first product label, adopted in 2014, for digital safe services. Since 2012, 29 labels have been issued by the CNIL.

Compliance packs

Following a broad discussion with the professionals concerned, different sector packs have been created: the “insurance” pack, the “social housing” pack, the “smart meters” pack and the “local authorities” pack.

Recommendations

The CNIL issued several recommendations in 2013, laying down for professionals the practical conditions for implementing the Data Protection Act. These recommendations related respectively to cookies and other tracers, the conservation of bank card data by retailers, and digital safes.

Advice for public authorities

In 2013, the CNIL issued 74 opinions on draft decrees or acts, including:

- the draft consumer act, with provisions for the introduction of a national personal loans register;
- the transparency of links of interest in the healthcare sector;
- the transparency of political life;
- the PNIJ (*Plateforme nationale des interceptions judiciaires* - national platform for judicial interceptions): regulatory text not yet published;
- the draft law on the use of geolocation as part of criminal investigations;
- the TAJ (*Traitement des antécédents judiciaires* - processing of criminal records);
- local public teleservices.

In addition, the CNIL provides members of parliament with its legal and technological expertise and suggests information and awareness-raising actions.

Support for innovation

Within the context of its innovation and forward planning activity, the CNIL is reinforcing its ability to listen and communicate with a large number of players from different backgrounds. This approach means that it can better anticipate technological developments and support new uses as far upstream as possible to guarantee sustainable innovation that respects the rights of users.

The CNIL therefore set up an innovation laboratory in 2013, which is used to test innovative products and applications, develop tools provided to the public, such as the Cookieviz tool, which has been downloaded 62,500 times, and coordinate research and development projects like the Mobilitics project, in partnership with Inria.

Monitoring notification of security breaches

Following the entry into force of the European Regulation on measures applicable to the notification of personal data breaches, in August 2013, the CNIL introduced a remote procedure, accessible from its website, to enable operators to submit notifications securely.

Facilitating the exercise of rights

Complaints

In 2013, the CNIL logged approximately 5,640 complaints, corresponding to a stabilisation of requests. This is mainly explained by better focussed requests, and by concentrating on practical content, specifying more precisely the circumstances in which the CNIL can intervene (e.g. practical sheets on personal data at work and on videosurveillance/protection).

Across all sectors, objection to appearing in a file is the main reason for complaint, as well as the exercise of the right to access. At the same time, 2013 confirmed the trend observed since 2011 regarding the high number of complaints relating to the “internet/telecoms” sector (34% of complaints received), and more specifically to the issue of e-reputation.

The CNIL received 1,917 complaints relating to the deletion of text, photographs, videos, contact details, comments, false online profiles, reuse of data publicly available on the internet, etc.

Right of indirect access

The CNIL received 4,305 requests for indirect access rights, a 17% increase compared to 2012. These demands represent a total of 7,148 checks to be carried out concerning, in order of importance, the tax authority's FICOBA form (*Fichier des comptes bancaires et assimilés* - bank accounts and similar file), criminal records (single TAJ form from 1 January 2014) and intelligence checks.

Sanctions

On 10 June 2013, the Chair of the CNIL sent a letter of formal notice to Google Inc. The office of the CNIL (the Chair and the two Vice-Chairs) decided to make this decision public, in particular due to the status and size of the organisation involved, and the number of people affected by its processing.

This letter of formal notice followed Google Inc.'s decision to merge into a single policy the various confidentiality rules applicable to around sixty of its services.

In her decision, the Chair of the CNIL maintained in particular that Google Inc. did not give its users enough information about the conditions under which their personal data was collected.

The company was also reproached, at the end of an inspection of proportionality between, , its legitimate interest on the one hand and, the rights and interests of internet users on the other, for not having obtained the consent of users before proceeding to combine their data. The Chair maintained that the size and the extensive nature of the data combination was susceptible to overlooking the right of users to respect for their privacy.

Other shortcomings relating to the duty to set a period for retention of the data collected or to inform users before placing cookies on their computer were also mentioned.

As the company did not comply as a result of this formal notice, a sanction procedure was launched. On 3 January 2014, the restricted formation of the CNIL declared a financial penalty of €150,000 and also ordered Google to publish a press release relating to this decision on www.google.fr.

On 14 January 2014, Google requested the partial suspension of the sanction deliberations against it by the restricted formation of the CNIL. The interim judge of the Council of State rejected this request in an order dated 7 February 2014.

Supervising the extra-territorial application of the laws of third-party States affecting European citizens

Mass surveillance systems

From March 2013, even before Edward Snowden's revelations were published in the press, the CNIL set up a working group responsible for holding hearings and reflecting on the question of access by foreign authorities to the data of European citizens.

The CNIL actively participated in the Article 29 Working Party (WP) preparatory work on mass electronic surveillance programmes. In this regard, it met with its counterparts in July 2013 to discuss the matter.

The Chair of the CNIL was also heard in October 2013 by the LIBE Commission of the European Parliament as part of discussions organised on the relevance of legal tools for supervising transfers in the Prism case.

This issue is not only linked to data protection, but raises considerations outside the limits of the powers of national data protection authorities.

For these reasons, the CNIL considers that one possible solution should be the creation of a specific tool, in the form of an international agreement intended to guarantee that the intelligence agencies of third-party countries offer an adequate level of protection.

However, under no circumstances may such an inter-governmental agreement legitimise a mass electronic surveillance programme such as Prism, within the outlines that seem to define the latter, given the information made public. Such an agreement should in fact be in line with the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (ECHR). This means in particular that any breach of the privacy of citizens must be strictly and demonstrably necessary, justified by a legitimate and proportionate purpose.

Furthermore, the CNIL supports the reintroduction of the former Article 42 of the original draft into the text of the draft European Regulation on data protection. This text indeed provided that transfers of data to countries outside the European Union in response to a request from a foreign authority can only be performed with the authorisation of the national data protection authority.

Blacklists

The CNIL has examined in more detail certain laws that create and impose on authorities and companies the obligation to check that their employees, suppliers or subcontractors are not on “blacklists” for various reasons.

Indeed, for several years some States—for instance the United States of America—have been seeking to protect themselves against various risks (for example, combating the funding of terrorism and strategically sensitive exports) through legislation laying down commercial exclusion sanctions or certain restrictions.

Management of these risks has resulted in the creation and use of international or national blacklists designating certain States, natural persons or legal entities, bodies or groups of companies as having to be the subject of a ban (for example, a ban on trading) or as requiring special attention. This legislation often requires that each operation directly or indirectly involving these countries, persons, entities, bodies or groups be inspected.

The CNIL has begun its reflections and recommends that a certain number of minimum precautions be taken with regard to the use of such lists.

Regulatory developments

The proposed changes to the Data Protection Act within the context of a draft digital law

Following the government's announcement in February 2013 regarding the submission of a draft digital law, the CNIL formulated several proposals for legislative change that could be anticipated in view of this draft.

These proposals concern the four main players in the data protection ecosystem: individuals, companies, public authorities and the CNIL.

In particular, the CNIL suggests:

- reinforcement of the effectiveness of personal rights (e.g. exercise of rights electronically, etc.) and specific protection for minors;
- continuation of the simplification of procedures for companies;
- extension of the CNIL's inspection authority to intelligence files, in accordance with conditions taking into account their specific nature;
- direct access to the data contained in criminal records for defendants (victims, plaintiffs);
- an increase in the maximum penalties and quicker triggering of a financial penalty procedure.

Participation in work on the European Regulation proposal

Given the size of the technological, political, economic and international challenges represented by the draft Regulation, the latter was the subject of much debate in 2013 in the European Parliament and in the EU Council.

In this context, the CNIL has continued its approach to raise public authority awareness of its concerns.

Regarding the one-stop shop, the CNIL has endeavoured to promote a balanced governance model, in everybody's interest. It has thus designed, in close partnership with the French government, an alternative and credible solution to the one-stop shop as proposed by the European Commission. This alternative proposal is based on the following elements:

- joint and shared competence for "transnational" processing between the authorities in the country of residence of the data subjects and the authority in the country where the company has its main establishment;
- organisation of cooperation between the data protection authorities through the appointment of a lead authority based on the criterion of the main establishment;
- adoption of the decisions within the context of a joint decision procedure;
- effective judicial remedy, for data subjects, before the judge in the State of their residence against the decisions of their authority and, for data managers, before the judge in the State of the lead authority to which their main establishment is answerable;
- a new role for the European Data Protection Board (EDPB) responsible for settling disputes between protection authorities.

On pseudonymised data, although the CNIL deems that the pseudonymisation of data, as a security measure, can justify a system of reduced obligations for data managers, it does however warn against the creation of special arrangements for pseudonymised data as it is.

On the risk-based approach, the CNIL considers that the risk-based approach must not, under any circumstances, affect the rights or result in the data controller (or the processor) being released from its general obligation to comply with the provisions of the regulation.

Organisation	French Data Protection Authority
Chair and/or College	Chair: Isabelle FALQUE-PIERROTIN Vice-Chairmen: Marie-France Mazars (since February 2014), Eric Peres (since February 2014). 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 2013 (in million €): 16.9
Staff	Number of staff: 178
General Activity	
Decisions, opinions, recommendations	2 542 decisions / 129 opinions / 3 recommendations
Notifications	92 351 notifications to the CNIL, including : 11 085 notifications for video surveillance systems 5 483 notifications for geolocation systems 29 Labels
Prior checks	Authorisations: 2 615 in 2013, including: 247 authorisations adopted in the Plenary, 1 078 data transfer authorisations to non EU States, 3 framework authorisations, 416 authorisations for biometric systems , 656 authorisations for processing of personal data for the purpose of medical research, and 215 authorisations for processing of personal data for the purposes of evaluation or analysis of care and prevention practices or activities
Requests from data subjects	Requests from the public: In 2013, the CNIL received 35 524 written requests and 124 595 calls
Complaints from data subjects	The CNIL received 5 640 complaints in 2013 Requests from data subjects: 4 305 requests for indirect access where processing involves State security, defence or public safety

Advice requested by parliament or government	In 2013, the CNIL adopted 129 opinions. Furthermore, the CNIL had meetings and was heard more than 20 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	414 investigations, including 130 investigations related to video surveillance systems.
Sanction Activities	
Sanctions	14 Sanctions taken by the CNIL in 2013. Legal actions against data controllers 56: (57 formal notices to comply, 7 financial penalties, 5 warnings), 1 discharge.
Penalties	Total amount 43 000 €, imposed by the CNIL in 2013
DPOs	
Figures on DPOs	12 953 bodies appointed a DPO in 2013 which represent 3 679 DPO

B. Information on case-law

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

- CE, sub-section 10, Mr B. A. v. CNIL 345408 (4/11/2013)
- CE, Interim Judge, SAS Paris Saint-Germain football & SASP Paris Saint-Germain handball v. CNIL 373061 (20/11/2013)
- CE, sub-sections 10 and 9 assembled, Mr B. A. v. CNIL, 328634 (3/06/2013)
- CE, Interim Judge, Mr B. A 365459 (14/02/2013)
- CE, Sub-section 10, Langlois, Association Internet sans Frontières, the company Ovh Sas v. SGG, Ministry for the Economy and Finance 347349 (20/11/2013)
- CE, Sub-sections 10 and 9 assembled, Mr A. / Council of State 359417 (17/07/2013)
- CE, Sub-sections 10 and 9 assembled, La Poste / Council of State 342372 (17/04/2013)
- CE, Sub-sections 10 and 9 assembled, Health, Safety and Working Conditions committee (CHSCT) of the company Lyondell Chimie France v. Ministry for the Interior 337982 (24/04/2013)

- Paris Court of Cassation, Commercial Chamber, SARL Google France v. the Cobrason company 1121011112471394 (29/01/2013)
- Court of Cassation, 1st Civil Chamber, company Agence du Palais v. Rose Marie V, 1119530 (10/04/2013)
- Court of Cassation, 1st Civil Chamber, company Google Inc. et al v. Société Lyonnaise de Garantie 1217591 (19/06/2013)
- Court of Cassation, Commercial, Financial and Economic Chamber, Mr X. v. the company Bout-Chard 1217037 (25/06/2013)
- Court of Cassation, Criminal Chamber, Mohamed X. v. Public Prosecutor 1381945 (22/10/2013)
- Court of Cassation, Criminal Chamber, company Biotronik France 1280346 (24/04/2013)
- Court of Cassation, Social Chamber, *Association départementale pour la sauvegarde de l'enfance, de l'adolescence et des jeunes adultes des Alpes-Maritimes* (ADSEA 06 - Alpes-Maritimes departmental association for the protection of children, adolescents and young adults) v. Mr CARTON, 1126099 (23/04/2013)
- Court of Cassation, Social Chamber, Mr Dubos v. the company Distribution Casino France 1216564 (26/06/2013)
- Court of Cassation, 1st Civil Chamber, *Union fédérale des consommateurs de l'Isère* (consumers' association) v. Caisse régionale de Crédit agricole mutuel Sud Rhône-Alpes 10283972 (23/01/2013)

GERMANY



A. Summary of activities and news

Federal Commissioner for Data Protection and Freedom of Information

Please note: In Germany there is not only the Federal Commissioner for Data Protection and Freedom of Information acting as Data Protection Authority. On the level of federal states (“Länder”) there are the offices of the Länder Data Protection Commissioners, and additionally, in Bavaria there is a separate supervisory authority with regard to the private sector.

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

Organisation	The Federal Commissioner of Data Protection and Freedom of Information
Chair and/or College	Mr. Peter Schaar (until 17 December 2013) and Ms Andrea Voßhoff ⁵
Budget	9 090 000 €
Staff	85
General Activity	
Decisions, opinions, recommendations	-
Notifications	-
Prior checks	-
Requests from data subjects	12 074
Complaints from data subjects	No distinction between complaints and requests
Advice requested by parliament or government	-
Other relevant general activity information	-
Inspection Activities	
Inspections, investigations	104
Sanction Activities	

⁵ Ms Andrea Voßhoff was elected as new Federal Commissioner for Data Protection and Freedom of Information by the German Federal Parliament on 19 December 2013 and took office after her appointment on 6 January 2014.

Sanctions	-
Penalties	0
DPOs	
Figures on DPOs	-

In the reporting period there were no significant changes or developments in Germany in respect of data protection at the statutory level.

The proposal from the OECD for a global information exchange to fight tax evasion and tax avoidance is one example of a development at the international level with consequences for implementation at the national level, and is described in more detail below.

The global financial crisis, the scandals involving so-called tax data CDs and the growing relocation of private assets abroad have led, at the international level, to the G20, the OECD, the Global Forum on Transparency and Exchange of Information and the EU taking decisive steps against tax evasion and tax avoidance.

On 20 July 2013 the Finance Ministers and the Governors of the G20 central banks approved an OECD proposal for a global model for automated exchange within a multilateral framework. The decision by the G20 also has to be seen in the light of the unanimous decision by the European Council of 22 May 2013, which gave priority to the expansion of the automatic exchange of information at the EU level and global level.

On 13 February 2014 the OECD presented a global standard for the automatic exchange of information. This specifies which information has to be shared and which financial service providers and taxpayers are covered. The international standard includes a model agreement, a Common Reporting Standard (CRS), comments on interpretation and minimum standards for IT solutions.

A period to mid-2014 is envisaged for work on a commentary to the standard. The Federal Ministry of Finance introduced the German data protection clause, including a custodial and capital punishment clause, into the discussion. The model developed at the OECD level is largely based on the intergovernmental approach for implementing the FATCA Treaty (Foreign Account Tax Compliance Act) initiated by the USA.

The G5 have now agreed to introduce the standard by the end of 2015 (FATCA plus one and a half years). This means that from 31.12.2015 financial institutions will have to examine their data in respect of existing accounts held by tax residents in other states and from 01.01.2016 will have to investigate the tax residency of the account holders according to a prescribed process (Due Diligence Procedure). The first report to the Federal Central Tax Office will then be made in September 2017. As part of the revision of the Administrative Assistance Directive, the European Commission is aiming to implement the so-called CAA/CRS (Competent Authority Agreement/Common Reporting Standard) within the EU without any change of content within the framework of European law.

The Federal Ministry of Finance believes that a CAA/CRS agreement should be implemented nationally by way of a Regulation, in order to simplify enactment. The statutory authorisation required for this would have to precisely determine the content, purpose and scope in accordance with Article 80(1) of the German Basic Law. Section 117c of the German Tax Code does not meet this requirement because it refers to an international agreement transformed into national law and the CAA/CRS is merely an administrative agreement. For data protection reasons in particular, a precisely specified statutory basis for an automatic exchange of information is required, however. The intention, therefore, is to add a

Section 117d to the German Tax Code, precisely defining the information to be exchanged, and the purpose and extent to which this information can be used.

This provision should take into account the principle of purpose limitation. Moreover, a guarantee of adequate data security should be secured by law with regard to the automatic exchange of information. Among other things, the form of guarantee for the data protection rights of the data subjects still has to be clarified. The possibility here is to insert a provision either into the enabling act or into the Regulation. The crucial point for the actual structure is that the data subject should have sufficiently transparent information about his or her rights as data subject.

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) made it clear as part of his response to the Federal Ministry of Finance that the national implementation of the CAA/CRS agreement to implement the new standard developed by the OECD for the automatic exchange of information affects the right to informational self-determination in Article 2(1) in conjunction with Article 1(1) Basic Law and therefore requires a statutory basis that corresponds to the constitutional requirement for clarity of legal rules, and is proportionate.

The implementation of the CAA/CRS agreement, which is classed by the Federal Ministry of Finance as an administrative agreement under international law according to Article 59(2) second sentence Basic Law, must be within the framework of statutory authorisation, which in this case still has to be created. In this case, it is necessary to give adequate consideration to the need for clarity in the specific instrument. For example, according to Article 80(1) second sentence Basic Law, the content, purpose and scope of the authority conferred must be specified in the enabling legislation. The Federal Commissioner agreed with the Federal Ministry for Finance that a separate legal basis (Section 117d German Tax Code) was required in order to satisfy the data protection requirements.

B. Information on case-law

Three judicial decisions were issued in 2013, dealing among other things with the applicability of German law to foreign internet providers. Some evaluative contradictions arose here. These include the following decisions:

Regional Court Berlin, 30.04.2013 (ref. 15 O 92/12)

In reviewing the contents of the data protection guidelines of Apple Sales International, Ireland, under the German Civil Code, the court checked the clauses used by the company on the processing of personal data. The provisions of the Federal Data Protection Act were applied as the standard of review.

Federal Court of Justice, 14.05.2013 (ref. VI ZR 269/12)

The court ruled on a claim by the injured party against the US-based search engine operator Google calling for the removal of specific search engine suggestions (the "Autocomplete" function) which were in breach of privacy rights.

3. Higher Administrative Court of Schleswig, 22.04.2013 (ref. 4 MB 11/13)

In a non-contestable ruling, the court found that Irish data protection legislation exclusively, rather than German law, applied to data processing by Facebook Ireland Limited, also in respect of German users. This was on the grounds that Facebook Ireland Ltd. is a branch office of Facebook in Europe.

C. Other important information

After the surveillance activities of the USA and UK became public the Federal Commissioner for Data Protection and Freedom of Information invited them to a meeting of the Committee for Internal Affairs last summer. During this meeting important data protection issues were discussed.

He also delivered a written statement about this issue to all members of parliament in a hearing in November 2013. This statement was included in the official documentation of the parliament (BT Drs. 18/59). Awareness regarding data protection issues could be raised in this way.

GREECE



A. Summary of activities and news

The Hellenic Parliament passed Drug Law 4139/2013, which, amongst other issues, comprises certain provisions regarding the publication of offenders' personal data and thus brought about changes in the Law 2472/1997 on personal data protection.

The HDPa issued in total 158 decisions and 6 opinions, some of which are presented in Section B "Information on case law".

Moreover, the HDPa expressed in writing its views on a) the personal data processing by credit rating agencies, b) on the two draft agreements - "Statement of Protocol" and "Memorandum of Understanding" - between the Hellenic Accounting & Auditing Standards Oversight Board and the U.S. Public Company Accounting Oversight (PCAOB) for the trans-border exchange of information related to the oversight of Auditors, c) the Hellenic National Action Plan for Open Government in the framework of Greece's participation in the Open Government Partnership (OGP) and d) the "Cl@rity" Program (<http://diavgeia.gov.gr/en>) according to which all ministries and public entities in general are obliged to upload their decisions on the internet.

On European Data Protection Day 2013, the HDPa posted on its website the brochure and video "Take control of your personal data" created by the European Commission (DG Justice) and useful information related to the reform of data protection legislation. Moreover, celebrating its 15th anniversary and aiming at raising awareness, the Authority organized a two-day conference the main theme of which was the contribution of the Hellenic DPA to the creation of a data protection-friendly environment in Greece.

The Authority also published four issues of its quarterly e-newsletter which features current developments in the field of personal data on a national, European, and international level. Finally, the HDPa posted on its website the results of the online survey on issues related to protection of personal data that had been conducted in 2012.

As to operational problems of the HDPa, once again, the serious problem of understaffing which the HDPa has been going through since its establishment could not be addressed in 2013 due to the prolonged difficulties in Greece's public finances. Additionally, the continuous decrease of the budget that is being granted to the HDPa for operational needs has restrained the Authority's ability to completely and sufficiently meet its obligations.

Organisation	
Chair and/or College	Petros Christoforos (President of the College).
Budget	€1 816 500.
Staff	Auditors Department: 14 lawyers and 11 IT experts (of these: three (3) on unpaid leave, two (2) on maternity leave); Communication and PR Department: 5 (of these: one (1) seconded for part of the year to another civil service and then transferred there, one (1) on maternity leave for part of the year, one (1) resigned due to retirement); Human Resources and Finance Department: 16 (of these: one (1) transferred to another civil service body, one (1) that seconded to the HDPa was transferred from another civil service body and one (1) on maternity leave, three (3) were also transferred from another civil service body and of them one (1) on unpaid

	leave).
General Activity	
Decisions, opinions, recommendations	The HDPa issued 158 decisions and 6 opinions.
Notifications	The HDPa received 650 notifications (381 concerned installation and operation of CCTVs and 92 data transfers to countries outside the E.U.).
Prior checks	The HDPa issued or renewed 127 permits concerning processing of sensitive data, interconnection of files and data transfers to countries outside the E.U..
Requests from data subjects	1 144.
Complaints from data subjects	692 (Prosecution Authorities and Public Order: 20, Public Administration and Local Government: 19, National Defence: 5, Taxation-Ministry of Finance: 3, Health: 5, Social Security: 13, Education and Research: 9, Banking: 111, Private Economy: 107, E-communications: 264, Work Relations: 22, Mass Media: 3, Other: 111).
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 2013, the HDPa posted on its website: the brochure and video “Take control of your personal data” created by the European Commission (DG Justice), useful information regarding the reform of data protection legislation. Additionally, celebrating its 15 th anniversary and aimed at raising awareness, the Authority organized a two-day conference (23-24 May) at the Athens Concert Hall. The main theme was the contribution of the Hellenic DPA to the creation of a data protection-friendly environment in Greece. The Authority also published four issues of its quarterly e-newsletter which features current developments in the field of personal data on a national, European, and international level. Finally, in 2013 the HDPa posted on its website the results of the online survey on issues related to protection of personal data that had been conducted in 2012.
Inspection Activities	
Inspections, investigations	10 inspections to data controllers in the private sector. More specifically, four (4) were conducted to companies so that their practices be investigated in regard to the lawfulness of the collection and processing of personal data in the framework of the provision of credit rating services. Two (2) additional inspections were conducted on two banks in regard to alleged data breaches that were, however, not substantiated. Two (2) more inspections were conducted on spam and the sending of unsolicited email for

	the promotion of services and goods by two companies. Finally, two (2) inspections were conducted on the operation of CCTV systems in a working place (pizza delivery chain) for the surveillance and the monitoring of workers' behavior and performance. The Authority also assisted the Cybercrime unit of the Hellenic Police in two cases (alleged data breach in a company and illegal processing of personal data obtained by means of a website).
Sanction Activities	
Sanctions	26 sanctions (6 warnings, 20 fines) were imposed by the DPA. It is noted here that in six (6) decisions the HDPa imposed a warning and a fine. The sanctions were related to the following thematic areas: Public Sector (3), Marketing – Promotion of goods and services (3), Financial Sector (4), Personal Data Breaches (2), Mass Media (1), CCTV (2), Education and Research (1) and E-communications (10).
Penalties	Fines: the total amount imposed by the Hellenic DPA was €311 735.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Opinion 2/2013

An opinion was delivered by the HDPa with regard to the posting on the Mutual Health Fund of Journalists' (E.D.O.E.A.P.) website regarding natural persons' debts related to insurance contributions and advertising tax. In response to a query submitted by the Mutual Health Fund of Journalists, the Authority deemed that the aforementioned Internet posting of the natural persons' debts doesn't constitute lawful processing of personal data. More specifically, it is not provided for by a law or a presidential decree and also doesn't comply with the principle of proportionality.

Opinion 4/2013

The Authority judged that the collection and processing of employees' penal record certificates by the insurance company they are working for does not constitute lawful processing, since it does not comply with the principle of proportionality. Alternatively, the Authority deemed that a solemn declaration would suffice.

Opinion 5/2013

The Authority examined a query submitted by the General Secretary for Public Revenue concerning a Draft Ministerial Decision on the system of bank and payment accounts registers that is under development. More specifically, this system aims at facilitating the transfer of bank secrecy waiver requests from the competent judicial authorities and services to financial institutions and the direct reception of the relevant replies without intent to breach the legislation about waiving the bank and professional secrecy. The HDPa deemed that the processing should be provided for by a law or a presidential decree in which the controller, the objectives, the data, the retention period, the recipients to

whom the data are communicated, the technical specifications of the applications required for the operation of the system, and the organizational and technical measures for the security of personal data processing will be stated. The Authority also judged that “sensitive information” should be deleted from the system upon the reception of the reply from the competent public authorities and services, and that additional technical measures should be applied to ensure that data replies are received by the requesting authorities. Finally, it concluded that the most appropriate solution for the protection of personal data and provision of effective remedy is that the financial institutions and not the General Secretariat for Information Systems of the Ministry of Finance (G.S.I.S.) have the obligation of data retention and also that the retention time should be specified so as to comply with the principle of effective remedy. In addition, the controller must notify the Authority about the intended processing before it begins.

Decision 42/2013

Following complaints and after carrying out administrative audits, the HDPa imposed a fine of €2,000 to a company for illegal collection and further use of personal data for the purpose of direct marketing and advertising by sending unsolicited electronic communications. Also, the Authority imposed the destruction of the file of email addresses. The amount of the fine was determined after taking into consideration, inter alia, the difficult economic situation of the company and the cooperation of its representatives during the administrative audit conducted by the Authority.

Decision 109/2013

With its Decision 109/2013, The Hellenic DPA imposed a fine of €75 000 to a bank for having purchased and maintained records of illegally collected personal data for the promotional activities of the bank. In particular, the data were collected without the consent of the data subjects and they were not obtained from publicly available sources that are intended to provide information to the general public nor had the subjects themselves disclosed their data for similar purposes - and all the above were known to the bank. The Authority also ordered the destruction of any relevant bank lists. By the same decision, the HDPa issued a recommendation to the bank to comply with the provisions of Article 11 of Law 3471/2006 **on the protection of personal data and privacy in the electronic telecommunications sector**, as amended and in force, concerning the promotion of products and services and the relevant Acts and Regulations instructions of the Authority.

Decision 58/2013

The HDPa judged that the processing of simple and sensitive personal data of people with disabilities for the purpose of exemption from payment of toll fees is a legitimate purpose of processing. However, the collection and maintenance of personal data of people with disabilities in the Special Exception Request form as it is used until now, constitutes unlawful processing of personal data. The company should collect less personal data in order to exempt disabled people from paying toll fees and also ensure that people with disabilities are informed about the collection of personal data and the confidentiality and security of processing.

Decision 98/2013

The HDPa imposed the highest possible fine on the General Secretariat for Information Systems (G.S.I.S.), judging that it violated its obligation to take appropriate security measures, something that resulted in a particularly serious incident of personal data leakage - that is, a data breach that involved nearly the total number of tax payers in Greece. The Authority ruled that the G.S.I.S., despite the bulk of data it manages and their critical nature, didn't have appropriate technical and organisational security measures in order to avoid the illegal access and dissemination of data until July 2013, or measures for the identification of potential incidents of a personal data breach.

Decision 136/2013

The Authority ruled that the provision of the service Street View by Google, Inc. is lawful - under the conditions laid down in the Decision 53/2011 - concerning the service Google Maps, and under specific conditions, namely, informing subjects before the start of data processing and satisfying the rights of access and objection. The company will have to satisfy these rights within a deadline of five days.

Decision 138/2013

The Authority inspected the Electronic Prescription System, with respect to the protection and security of personal data. As the operation and maintenance of the ePrescription system is fully contracted to a company supervised by the General Secretariat of Social Security (hereinafter, GGKA), the conduct of the inspection took place entirely on the premises of IDIKA and its subcontractors. The HDPa asked the data controller, i.e. GGKA, to submit, within two months from the date of the decision, a detailed timetable for the implementation of the recommendations set out in the grounds of the decision, as well as to address specific issues placed in the confidential annex. The schedule should also cover all the remedies provided in the ongoing call for tender for the new Electronic Prescription System which have not yet been taken. Furthermore, the Authority asked the controller to submit quarterly reports with regard to the work progress. Finally, the HDPa asked the controller to describe in the application to be submitted for renewal of the permit of processing sensitive data files in regard to the new measures that will have been taken in the meantime.

CCTV systems:

Decision 49/2013

Three private schools installed CCTV systems to avoid theft and vandalism on their premises and safeguard the safety of pupils and employees. These schools wished to operate the system 24 hours a day and requested to be excluded from the application of article 18 of the HDPa's Directive 1/2011 on the installation of CCTV systems, which sets out that video surveillance systems in schools can only operate during non-working hours. The Authority rejected their request, since these schools did not provide any new suggestions which would allow the non-application of this provision. Furthermore, what they required had already been taken into account by the HDPa at the time of drafting the aforementioned directive.

Decision 78/2013

In this case, the HDPa was called in to examine a parent's complaint concerning a kindergarten which had been operating a CCTV system in the classrooms, the yard, the entrance hall, and the director's office during the whole day, without having notified the parents or the Authority. The director of the establishment submitted a notification to the HDPa and explained that the reasons for having installed such a system were that the area of the premises was very big, that there had been several accidents regarding children, and that parents were duly informed. The HDPa deemed that the principle of proportionality was not respected and issued a warning to the kindergarten to uninstall the cameras from classrooms, to ensure that the cameras in the yard would be located at the perimeter thereof, that there would be no monitoring screens, and that data would be deleted on the following working day (except in case of incidents). Moreover, the HDPa advised the kindergarten to respect the access and objection rights.

Decision 59/2013

This was about a video surveillance system installed in a state building (city hall) to protect public property from acts of vandalism and, more specifically, a number of surrounding monuments, which during the last two years had been significantly damaged. The system was deemed necessary due to the fact that milder measures had already been used, such as better lighting and police patrols, and had not had the expected result. The HDPa invited the controller to modify the current CCTV system in such a way so as i) to focus only on the specific monuments, ii) to remove the monitors and keep only the recording system, iii) system passwords should be known only by a particular person, who would be appointed as head of security of the CCTV, iv) access to image data and installation of monitors would be possible only if an incident had occurred and upon a written order of the mayor.

HUNGARY



A. Summary of activities and news

In 2013, the National Authority for Data Protection and Freedom of Information (hereinafter: NAIH) received more than 3,000 submissions. The great majority of them were investigated with an informal procedure (investigation). The NAIH launched 40 formal (administrative) procedures, and imposed fines in 31 cases. Some of these decisions were challenged by data controllers before the court. The courts have upheld the vast majority of the examined decisions.

Organisation	National Authority for Data Protection and Freedom of Information
Chair and/or College	President: Mr. Attila Péterfalvi
Budget	467 500 000 HUF
Staff	56
General Activity	
Decisions, opinions, recommendations	<p><u>Administrative decisions</u></p> <p>In 2013, the Authority processed 40 Data Protection cases. At the time of the annual report's redaction, 4 of those were still pending. 35 of the 40 Data Protection cases resulted in an administrative decision. Some of the cases were still pending by the end of 2012.</p> <p><u>Opinions on draft legislation:</u> 311 cases</p> <p><u>Opinions on voice recording:</u> The NAIH noticed an increased trend in complaints related to voice recording activities. According to the Privacy Act, voice recordings constitute personal data insofar as they can be linked back to the data subject. Several laws provide for the mandatory recording of voice conversations. Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises provides that such institutions have to record complaints via phone. Insurance companies are bound to the same obligation, according to Act LX of 2003 on Insurance Institutions and the Insurance Business. These two acts indicate that data subjects must be given the opportunity, if they wish, to hear the recording of their voice. The NAIH's official opinion is that both parties have the right to access the voice recordings. The data subject's access to them must therefore also be ensured. They must be in a position to listen to the recording, and get a copy, free of charge, as a rule.</p> <p><u>Resolutions</u></p> <p>Our Authority issued 1 549 resolutions on specific data protection issues (informal procedures).</p>
Notifications	We handled 11 686 notifications of personal data processing to the DP register.
Prior checks	No data.

Requests from data subjects	These requests for intervention are treated as “consultative requests” which cover requests from data controllers and out of the 932 requests, 790 concerned data protection issues. 140 were related to freedom of information issues.
Complaints from data subjects	The NAIH received 1 239 complaints from data subjects. Out of the 1 239 complaints, 978 cases concerned data protection issues, and 261 cases concerned freedom of information issues.
Advice requested by parliament or government	The NAIH is consulted on a regular basis on draft legislations.
Other relevant general activity information	International cases: 106
Inspection Activities	
Inspections, investigations	<p><u>Data protection procedures</u></p> <p>Formal data protection procedures are launched ex officio. In most cases, formal procedures follow informal investigation procedures. The information gathered during the latter can be used during formal procedures.</p> <p><u>2013’s investigation strategy</u></p> <p>The Authority designated three areas that are of particular importance, and which are stated as its priorities for 2013:</p> <ol style="list-style-type: none"> 1. Data processing operations by websites, including the registration process from the point of view of users' rights. A strong emphasis was put on the processing of children's personal data. 2. The electronic disclosure of information on local taxes. 3. Personal data processing operations by debt management companies. <p><u>Investigation</u></p> <p>The main task of the Department of Investigations is to investigate incoming complaints. Besides this, it replies to the consultation requests it receives to help the enforcement of data protection guidelines.</p> <p><u>Audit</u></p> <p>In 2013, the Authority launched its Data Protection Audit service. Data controllers can, against the payment of a certain fee, ask for an audit. The NAIH conducted 10 audits in 2013.</p>
Sanction Activities	
Sanctions	The NAIH may impose several types of sanctions. During informal procedures, the NAIH may call on the controller to bring its

	procedure in line with the Privacy Act. During formal procedures the NAIH may order the rectification of any personal data that is deemed inaccurate, order the blocking, erasure or destruction of personal data processed unlawfully, prohibit the unlawful control or process of personal data, prohibit the transfer of personal data to other countries, or order the information of the data subject, if it was refused by the data controller unlawfully, and impose a fine.
Penalties	The enforcement of administrative fines is part of the Authority's responsibilities. These are the main figures of this activity in 2012-2013 : Number of cases 47: Fines imposed: 20 677 478 HUF
DPOs	Since 2012, according to its legal duties, the NAIH organises at least once a year the Conference of Internal Data Protection Officers.
Figures on DPOs	The DPA keeps a register on DPOs. In 2013, more than 400 DPOs were registered in the database, which is used to invite all interested DPOs to the Conference.

B. Information on case-law

Relevant cases

A) Investigations into data processing operations by websites, registration processes, and the enforcement of data subjects' rights on the Internet, especially those of children

The NAIH undertook an overall investigation into data processing operations by certain websites, in order to evaluate privacy policies, registration processes, the scope of processed data, and the enforcement of data subjects' rights. In the framework of this procedure, the NAIH gave special attention to the processing of children's data. The importance placed on minors as data subjects during our procedure was justified by the fact that, contrary to the former Data Protection Act, the new Privacy Act, in its article 6 paragraph 3, provides that children over 16 have the right to consent to data processing operations independently of their legal guardians.

To determine the validity of legal statements and minors' consent to data collection, it is also necessary to take Act IV of 1959 of the Civil Code (hereinafter: the Civil Code) into account. According to article 12/C paragraph 1 of the Civil Code, only a minor's legal guardian, as his legal representative, may make legal statements in his name. According to article 12/A, paragraph 2, of the Civil Code: "legal statements by minors enjoying limited legal capacity are valid only if accompanied by their legal representative's prior or subsequent consent, unless provided otherwise by other laws". Such derogation is provided by article 6 paragraph 3 of the Privacy Act. By this provision, the legislator created special rules for minors between 16 and 18 years old, but for minors between 14 and 16, consent by both the data subject and his legal guardian remains necessary, as provided by the Civil Code's main rule.

The NAIH encountered the case of a company operating several types of websites, including dating websites where it was usual to find registered users under the age of 16, who were able to register despite the absence of their guardians' either prior or subsequent consent. The NAIH investigated several dating websites and observed that minors below 16 could frequently be found as registered users. According to the NAIH, it is important to place the child's superior interests into highlighted account when

examining their online activities and the data processing operations that concern them. This is particularly true in the case of social networks. Inside this category, dating websites represent the greatest threat. Indeed, unlike regular social networks where users communicate mostly with known friends, the main function of dating websites is to meet new people. Given that services provided by dating portals to minors, and the data processing operations they infer, do not fall under the category of small everyday acts that are usual and necessary to fulfil the child's basic needs, the NAIH believes that adequate consent can only be constituted along with the legal guardian's consent, and not only the child's.

One must strive to enforce the aforementioned rules even if it is truly difficult to verify parental consent. Otherwise, the website's owner or operator facilitates the availability of children for romantic or sexual relationships, which can contribute to their victimization.

We cannot close our eyes to the fact that children can appear on dating websites and be available on websites created to promote the establishment of new relationships. We cannot ignore, and thereby passively approve, such practices. This needs to be asserted even despite the knowledge that registration rules and processes can easily be circumvented. In that case indeed, the problem lies not in the data controller's behaviour, but in the field of child-parent relations, and becomes part of a larger social problem.

This is why the NAIH investigated the registration processes of no less than 50 dating websites. The NAIH tried to establish whether it was possible or not for minors to register without parental consent. Over the course of our test registrations, the NAIH was led to launch administrative data protection procedures against 18 websites. In total, about 4200 profiles were found of minors below 16. The youngest user was only 10 years old. All of those profiles were available online, with the aim of establishing relationships. As a result, the NAIH imposed fines amounting to 2 900 000 HUF in total, and forced data controllers to erase relevant data and change their data protection policies.

Over the course of the procedures, data controllers were globally cooperative, and deleted the illegally processed personal data, that is to say, the profiles of minors below 16. They modified their procedures and raised the registration age limit accordingly.

B) The construction of a common marketing database

The NAIH investigated, in the framework of an administrative data protection procedure, the data processing operations of two companies operating marketing databases. The source of the collected data was registration of the companies' websites. The two companies transferred and shared the collected data between one another, and sent emails and SMS messages to the registered users. Telemarketing activities were conducted at a sub-contractor's call centre. Their aim was to advertise various banking and insurance products. Their partner would call people using the company's identity, to promote their own offers or those of others to people registered in either of the two companies' databases. Personal data was therefore received and used by the call centre, and not by the original data controllers collecting the data.

The NAIH established that the investigated operations did not adequately comply with information requirements, and that the operation's indicated purpose ("marketing purpose") was too vague. There was a total lack of legal basis, for instance the data subjects' consent, for the transfer of personal data by both companies to a partner that was not even named in the general terms and conditions. Both data controllers also failed to provide adequate and precise information and ask for deliberate opt-in. Furthermore, the notification sent to the NAIH for prior registration purposes failed to mention all the involved agents.

Given the established infringements, the NAIH decided to impose a fine, request the adaptation of privacy policies and data protection practices to the Privacy Act's requirements, and require the deletion of illegally collected data.

C) Data breach following a hacker attack

A company collected personal data in the framework of a lottery game for direct marketing purposes, with the data subjects' consent. On its website, the company also gave registered users access to a 3D game. After the marketing campaign was over, the data controller left an active link pointing to the database on its website. A group of hackers intruded on the database server. They uploaded the stolen data on several websites, including names, e-mail addresses, phone numbers, dates of birth, city names and, in some cases, the passwords. This data breach concerned more than 50 000 people.

Given the economic size of the data controller, the NAIH considered it to be its responsibility to implement the most efficient data security measures. This charge was aggravated by the fact that internal audits already brought attention to the fact that, especially in the face of remote access, these data were not adequately protected.

D) Biometric systems

In regard to cases concerning biometric systems, some were consultation requests by organisations contemplating the introduction of biometric locks or entrance systems. Following its usual standpoint, the NAIH stressed that, given the provisions of article 4 of the Privacy Act, it is necessary for the use of biometric systems to be adequate, relevant, and proportionate. This infers the requirements for the necessity of the use of such data, its proportionality, and the strict evaluation of whether or not it would be possible to achieve the same goal by other, less intrusive means. Furthermore, the NAIH continued to base itself on the conclusions contained in Opinion 03/2012 of the Article 29 Working Party on the development of biometric technologies, and especially those related to how the proportionality of such processing operations should be evaluated. According to such principles, projects by schools to introduce biometric entrance systems are a continuing concern. Indeed, such systems are not indispensable to either the safety of interested parties or that of school property. Finally, the desired purpose of such a system can be attained by less invasive means.

The NAIH also examined cases where undertakings wished to implement a fairly common device, a fingerprint reader, on cash registers, to limit their access to authorized personnel. The NAIH reminded such companies that, according to article 10 paragraph 1 of the Labour Code, "only declarations or data relevant to the establishment of labour relations, the carrying out of this relation, or its termination, can be requested from an employee, and only as long as such requests do not violate his civil rights".

Article 9 of the Labour Code provides for the general rules and main principles on the scope of employees' civil rights in labour relations, and on their potential restrictions. In order to protect such civil rights, the Law provides for two strict procedural obligations employers must respect. This procedure must be exclusively and directly tied to the employer's proper functioning. It may not exceed these boundaries. Even the notion of proper functioning is to be strictly interpreted. The employer may only decide to undertake such a procedure if it is obviously and objectively necessary.

Based on the above, the NAIH established that the implementation of fingerprint readers on cash registers was not proportionate, as the purpose it fulfils can be attained through less invasive means in terms of civil rights, like cash registers with increased safety that could only be opened by the use of a special code, given by the employer to its authorized employees.

C. Other important information

Statistics

In 2013, the Authority received over 5 700 postal and 11 222 electronic mails. We furthermore processed 11 686 notifications of personal data processing, of which 7 420 arrived by postal mail, and 4 266 by e-mail. We opened 3 280 cases in 2013, which represents a 9 % rise from 2012 figures.

Among those cases, we launched 40 administrative procedures and 2 481 investigation procedures. The remaining 759 cases pertained to other branches of our activity, such as international affairs or relations with data protection officers. Only 370 of the investigation cases started in 2012 had to be continued in 2013. In January 2014, the number of unfinished cases from the previous year dropped to 341. We managed to complete 90 % of our procedures in 2013, which constitutes a significant achievement in a context of rising case numbers. We also dealt with 106 international cases.

Key to the world of the Net!": the NAIH's children protection project

In 2013, the NAIH launched its first long-term project. Its topic constitutes one of our top priorities: the protection of children's rights in an online environment. The first step of this project was to realize a comprehensive study on young people's use of the Internet, the dangers they face in an online environment, and the relevant legal regulations both in Hungary and abroad. We conducted our study with the cooperation of various national and international partners. Our aim was to include in our work the help of experts in education, psychiatry, law, criminology, and information technology, as well as to gain information on the best international practices. No less than 12 experts were involved in the writing and publication of a 122 page study, and an informational leaflet was designed for children and presented in several schools in Hungary. This document was translated into English, and a short summary was also made available in French. Both can be freely downloaded from our website: www.naih.hu. It is our aim to pursue this project with our international partners in the framework of an international workshop on digital education, under the leadership of the French Data Protection Commission (CNIL), and of a project funded by the European Union called "Introducing data protection and privacy issues at schools in the European Union", under the leadership of the Polish Inspector General for Data Protection (GIODO).



IRELAND

A. Summary of activities and news

In 2013, the Office of the Data Protection Commissioner opened 910 complaints for investigation (many complaints are dealt with informally by providing the complainant with appropriate information on their rights). 1 290 investigations of complaints were concluded in 2013. As in previous years, the vast majority of complaints were resolved amicably, with only 29 complaints giving rise to formal decisions. Prosecutions were taken against companies for marketing offences under the Privacy in Electronic Communications Regulations (S.I. 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 2013 is included in section B of this report. Notifications of personal data security breach notifications to the Office remained at a consistent level (1 507 in 2013), continuing to reflect the trend since the introduction of the Personal Data Security Breach Code of Practice in 2010. In one major data security breach involving a data processor based in Ireland with contracts with a number of data controllers across Europe, the Commissioner issued an enforcement notice preventing the data processor concerned from processing data until they had met certain requirements in relation to data security. The Office also implemented an on-line form to enable the reporting of breach notifications by telecommunications and internet service providers in line with the requirements of European Commission Regulation 611/2013.

Organisation	Office of the Data Protection Commissioner
Chair and/or College	Billy Hawkes
Budget	€1 727 000 budget. €1 960 999 expended.
Staff	30 as of 31 December 2013
General Activity	
Decisions, opinions, recommendations	29 formal decisions
Notifications	5 778
Prior checks	N/A
Requests from data subjects	12 000 email queries. Also queries in writing.
Complaints from data subjects	910
Advice requested by parliament or government	Regular informal consultation on legislative/regulatory proposals
Other relevant general activity information	1 507 data security breach notifications.
Inspection Activities	
Inspections, investigations	44 audits (inspections)
Sanction Activities	

Sanctions	101 prosecutions against 14 entities
Penalties	€35 600 fines imposed plus costs. €27 750 charitable donations ordered by the Court through application of Probation Act, plus costs.
DPOs	N/A
Figures on DPOs	

B. Information on case-law

In most cases, in accordance with section 10 of the Irish Data Protection Acts of 1988 and 2003, complaints submitted to the Commissioner are resolved amicably without the need to 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 one case (mentioned in section A above) an enforcement notice was issued preventing a data processor from processing data until certain requirements regarding data security were met. In some cases, data controllers are named in case studies included in the Commissioner’s Annual Report. In 2013, the Commissioner engaged in several successful prosecutions under Statutory Instrument 336 of 2011 (transposing Directives 2002/58/EC, as amended by 2006/24/EC and 2009/136/EC in Ireland) in relation to unsolicited marketing text messages and emails. 101 prosecutions against 14 entities were undertaken in 2013.

C. Other important information

The Commissioner continued to engage with large public sector organisations regarding data protection. The Office has now completed audits of three major State holders of personal data – the Department of Social Protection, the Revenue Commissioners, and An Garda Síochána (national police force).

An audit of data protection in An Garda Síochána took place from 2011 to October 2013. The report was published by An Garda Síochána in March 2014. A central focus of the audit was the main IT system used by An Garda Síochána for recording data, PULSE.

The audit findings highlighted areas where improvements are required. Overall, the majority of areas examined demonstrated a professional police force operating in compliance with data protection legislation.

In 2013, the Office also began a major audit of LinkedIn-Ireland.



ITALY

A. Summary of activities and news

Legislative Changes

Data Protection Code (Legislative Decree no 196 of 30 June 2003)

Section 19, para 3-bis of the Data Protection Code was repealed by section 53(1)(e) of legislative decree no. 33 of 14 March 2013. However, the wording of the paragraph in question was shifted to section 4(5) of the said legislative decree ("The information concerning performance of the tasks committed to any person that is in charge of public functions including the respective evaluation shall be made available by the public employer. Except where provided for by law, no information may be disclosed concerning the nature of the medical conditions and/or personal or family circumstances resulting from a person's absence from the workplace or the elements making up the evaluation or any information on the employment relationship between the aforementioned public employee and the public employer if they are suitable for disclosing any items of information referred to in section 4(1)d. hereof.").

The up-to-date version of the Data Protection Code is available in English at the following link: <http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf>

Main activities

Data processing in the public sector

The DPA gave its opinion (7 February 2013) on the draft legislative decree (adopted on 14 March 2013 – No. 14) which sets forth specific transparency obligations public bodies have to comply with (e.g. through publication on their institutional web sites). The Garante signaled some criticalities of the draft text and provided specific suggestions to reconcile transparency and the protection of personal data, such as: avoiding the dissemination of particular categories of data, namely those related to individuals' health; preventing the data published on line from being retrievable by means of general search engines such as Google (internal search engines are preferable); setting out the period during which posting of data on websites can be regarded as proportionate with a view toward achieving transparency; limiting the publication of data related to public sector employees to those data which are strictly relevant; in respect of holders of political offices, limiting the publication of data relating to holders of political offices by taking proportionality requirements into account.

Countering tax evasion

The DPA, following specific investigations, prescribed measures to be adopted in regard to the processing carried out by the Revenue Agency aimed at the concise assessment of individuals' income to counter tax evasion (21 November 2013). The measures were meant to ensure that the anti-fraud activity in question was carried out with due respect for the protection of personal data; they consisted, in particular, of specific adjustments to be made by the Agency regarding the criteria for taxpayers' profiling and for the selection of the individuals subject to investigations; furthermore, arrangements were laid down in regard to data quality; data retention; information to be provided to data subjects regarding the processing of data and the possibility of being heard by the Agency.

Justice

The DPA set out measures and arrangements that public prosecutor's offices in Italy will have to implement in order to enhance the security of any personal data they collect and use as part of intercepted communications (24 July 2013). The measures include both physical security measures

(such as access to premises only via individually allocated badges associated with a numerical code or biometrics-based devices; logging of all accesses; CCTV monitoring of the premises) and IT security arrangements (such as use of dedicated workstations and strong authentication procedures for operator access to systems and servers; logging of all interception-related activities; encryption-protected copying to removable media; encrypted storage of original records and back-up copies; use of secure network protocols for data exchanges between judicial authorities and ISPs).

Intelligence services

Following Edward Snowden's revelations, a Memorandum of Understanding was signed by the Italian DPA and the Department of Information Security of the Presidency of the Council of Minister (11 November 2013). The MoU aims at completing safeguards for individuals' rights concerning data processing for intelligence purposes with particular regard for the oversight by the Garante in regard to intelligence services and the mechanisms for assessing the activities performed by those services with regard to public sector databases and cybersecurity initiatives [namely in respect to the access to databases held by public bodies and the access for cybersecurity purposes].

Marketing

The DPA intervened on several occasions in the field of marketing. It issued Guidelines on marketing and against spam (including the so called social spam, viral marketing, and targeted marketing) laying down a consolidated set of measures and precautions that can be helpful both to the companies that plan a marketing campaign to advertise their products or services and to any individual wishing to fend off advertising without consent (4 July 2013). The DPA clarified, via a separate decision, that it is enough to obtain consent once for all marketing activities – such as sending ads or performing market surveys; the consent provided to receive automated promotional messages (emails, SMS-texting) also applies to such messages when sent via less privacy-intrusive channels such as paper mail or through operator-assisted phone calls, providing users are informed appropriately and enabled to freely express their respective preferences (15 May 2013). Detailed rules were set forth for public and private bodies planning to rely on call centers located outside the EU. In addition to recalling the requirements to be met for transferring personal data (in particular, customer data) to third countries, the DPA ordered the controllers concerned to provide specific information to their customers and afford them the option to select operators located in Italy in regard to incoming phone calls (10 October 2013). Specific measures were laid down by the Garante and submitted to public consultation to prevent silent calls, which are a major source of concern for users. The measures include, in particular, termination of silent calls (i.e. when no operator is available to take the call) within 3 seconds of pick-up by users; setting a threshold of 3 silent calls every 100 successful calls (per single telemarketing campaign); a ban on re-contacting a user before one week has elapsed from the silent call; and storage of statistics on silent calls for at least two years to enable oversight.

Profiling by Telephone Companies

Telephone companies were allowed by the DPA to perform profiling activities by relying on aggregate data over a shorter time period (two days rather than one month as was the case so far). The main reason behind this decision was the growing use of number portability options and the wider gamut of data offers (and profiles) available to customers. The aggregate data in question include originating and terminating traffic volumes (in minutes or bytes), number of recharges (per sales channel, i.e. online, ATM, debit cards) and total recharges. All the other safeguards as set forth by the DPA in previous decisions remain applicable - including the use of dedicated IT systems for profiling and stringent security measures for data access.

Mobile Payments

The DPA adopted a decision (12 December 2013) on mobile payments, setting forth specific safeguards to protect the personal data of users who, by directly charging their phone bills, make payments at a

distance using the so-called mobile remote payment systems. This payment mode is becoming increasingly widespread and entails the processing of several personal (at times sensitive) data such as census information, the type of service or product being purchased, and date and time of purchase. The safeguards – which include a specific information notice, consent in case of marketing and profiling; security measures, data retention policies – are addressed to the three main stakeholders involved in mobile payment services (the carriers, i.e. electronic communications providers; payment hubs supplying and managing the technological platforms for such services; the merchants offering and selling digital contents, multimedia and other products).

Google Street View

The DPA sanctioned Google with a 1-million-Euro fine because of Google's Street View service in December 2013 due to, in particular, a circumstance in which unlawfully collected information had been pooled into a large database – the one set up by Google in connection with the Street View service; furthermore, the Garante decided to rely on the provision in the Privacy Code that is aimed at ensuring effective sanctions are imposed on major business entities – given that Google's consolidated turnover for 2012 totaled over 50 billion dollars.

Data breaches

The DPA adopted a general decision, replacing previously adopted Guidelines, in pursuance of paragraph (6) of section 32-bis of the Code (implementing Directive 136/2009/EC) in order to provide guidance and instructions on the circumstances under which electronic communications service providers are required to notify personal data breaches, the format applying to such notification, and the relevant implementing arrangements (4 April 2013).

Graphometric authentication techniques

The DPA granted two prior-checking applications from banks intending to use graphometric authentication techniques for customer identification. The DPA requested that the purpose limitation principle should be complied with strictly and that fallback procedures be available for those users who do not wish or are not able to rely on this authentication method; data retention arrangements will also have to be compliant with the proportionality principle.

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 WPISP – Working Party on Information Security and Privacy (now renamed WPSPDE) 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 the 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).

At both the European and international level, the year 2013 was also characterized by the important work done by the DPAs to achieve closer and more effective cooperation, especially in the enforcement area through specific working groups in which the Italian DPA participated (GPEN, IECWG, Phaedra project, etc.). 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 until June 2013, FYROM), and European Neighbourhood Policy countries.

Organisation	Italian Data Protection Authority
Chair and/or College	Chair of the College: Dr Antonello SORO College: Ms Augusta IANNINI Ms Giovanna BIANCHI CLERICI Ms Licia CALIFANO
Budget	Approx. 8.4 million EURO (Funding by Government)
Staff	122
General Activity	
Decisions, opinions, recommendations	Number of decisions taken by the College: 606
Notifications	1 656
Prior checks	24
Requests from data subjects	Total number of requests: approx. 4 700 Requests for information ("quesiti"): 311 Reports and claims ("segnalazioni" and "reclami" received in 2012) from data subjects: 4 393
Complaints from data subjects	(formal complaints, specifically regulated by the DP Code, concerning access to one's personal data): 222
Advice requested by parliament or government	22
Other relevant general activity information	The front office of the DPA received, in 2012, about 31 000 telephone calls and emails
Inspection Activities	
Inspections, investigations	Number of inspections and/or investigations (on the spot): 411
Sanction Activities	
Sanctions	Approx. 850
Penalties	Amount: approx. 4 million EUR imposed by financial police in charge of controls on the DPA's behalf
DPOs	
Figures on DPOs	N/A

B. Information on case-law

Supreme Court – Google Vividown case – No criminal liability vested in a hosting service provider

The Italian Third Criminal Chamber of the Supreme Court (by its decision No. 8611/2013) published the reasoning for its verdict of acquittal for the three Google executives who were sentenced to six months in prison by a first instance judgment in 2010, following the upload on the Google video platform of a video in which a disabled minor was humiliated by classmates. According to the Supreme Court, Internet host providers cannot be held criminally liable in cases of violation of privacy due to videos posted on the web. This very important decision states that “the offences before us here, relating to Section 167 of the Privacy Code, shall be construed as offences committed in breach of one’s duties, as here we are dealing with conduct only resulting in a breach of the obligations of the owner of the data processed and not of any other person who in any way handles the data being processed, but without related decision-making powers”. The Supreme Court has also specified that the hosting service provider “has no control over the data stored nor does it contribute in any way to the selection of the same, its research or the creation of the file that contains it, such data being entirely attributable to the users of the service who upload them onto the platform placed at their disposal”.

Court of Cassation (Supreme Court) –The consumer has the right to be informed timely of negative reports concerning him

A decision by the Civil Division of the Court of Cassation (No. 349/2013) concerning consumer rights found that a consumer has the right to be informed in a timely manner of negative reports that concern them. The Court declared as inadmissible -for reasons relating to service of process - the action brought by a financial company against the judgment of the lower court in Milan. In this case, the data subject, having heard of a "negative report" against him that related to a loan he had been granted in 2003, had filed an appropriate request for access to the company's database in 2008 and then appealed to the Court of Milan when he had failed to receive a response. The Supreme Court confirmed the consumer's right to know promptly his or her position in the archives of the financial company, highlighting, in particular, that the data controller is required to verify the login request "without delay". Accordingly, the trial court had taken due account of the 15-day term set in the law for the controller to reply to access requests, finding that such a term was adequate for the controller to make a decision on the request.”

Court of Cassation (Supreme Court) - Unlawful interference with private life

The Criminal Division of the Court of Cassation (by its decision No. 8762/2013) rejected an appeal against the decision of the Court of Appeal of Florence who had sentenced the defendant for violation of article 615- bis of the Italian criminal code (cp.) after he had come to know about a conversation between his sister and his girlfriend in his flat by hiding a tape recorder in that flat. The Court, referring to settled case-law, said that the offense of unlawful interference in private life also exists in the case of unfair recordings such as the one in question, underlining that for the purposes of the applicability of art. 615 -bis of the Criminal Code, “one’s home (private dwelling place) includes the place where a significant part of one’s emotional life is led, even if not usually...”. The decision highlights that in such a place a person is usually confident of the protection of his/her privacy, and therefore particularly exposed and vulnerable against devious and unfair behavior by the person he or she is emotionally related to.

C. Other important information

The DPA expressed its interest in having the Italian State enter an appearance before the EU Court of Justice in case C-46/13 (request for a preliminary ruling under Article 267 TFEU) on interpretation of Article 7(c) of Directive 2006/24/EC. In particular, the questions asked by the Austrian Data Protection Commission to the EU Court of Justice were aimed at understanding, among others, if Article 7(c) of Directive 2006/24/EC can be interpreted as meaning that an individual who is a data subject of retained data does not qualify as ‘specially authorised personnel’ within the meaning of this provision, and has no

right of access to their own data from the provider of publicly available electronic communications services or of a public communications network. The Italian DPA underlined that, according to Sections 7 and 8 of the Italian Data Protection Code, data subjects can access all personal data referring to them as processed by a service provider, except for incoming phone calls, unless this may be actually and concretely prejudicial to performance of the investigations by defence counsel.

LATVIA



A. Summary of activities and news

Regarding the main developments, the amendments to the Personal Data Protection Law have been elaborated (in force since 7 March 2014). The amendments foresee clearer involvement of data subjects within the personal data processing in order to solve problems related to that (ex., in cases when the data subject asks for a large amount of information from the controller, etc.). Amendments also concern video surveillance – it is mandatory to notify the Data State Inspectorate of such data processing only in those cases where personal data that has been acquired from video surveillance is stored. There have been amendments to several sectorial laws that have increased the workload of the Data State Inspectorate, mainly regarding the notification of video surveillance to the Data State Inspectorate.

Considering the widespread use of video surveillance in Latvia, the Data State Inspectorate of Latvia has initiated a broader discussion on this topic along with the Ombudsman office.

Organisation	DATA STATE INSPECTORATE
Chair and/or College	Director – Signe Plūmiņa
Budget	In 2013 – 265 317 LVL (or 377 512 EUR)
Staff	19 (including administrative staff)
General Activity	
Decisions, opinions, recommendations	Decisions – no statistical data available; opinions – no statistical data available; recommendations - 2
Notifications	532
Prior checks	493
Requests from data subjects	6
Complaints from data subjects	362
Advice requested by parliament or government	No statistical data available; advice to the parliament or government often given by the Ministry of Justice which also includes the opinion of the Data State Inspectorate.
Other relevant general activity information	8 decisions by the Data State Inspectorate's officials have been appealed against to the director of the Data State Inspectorate. 4 decisions by the Data State Inspectorate's director have been appealed against at court. Main areas of the complaints: Violation of data subject access rights (both regarding the information to be provided when starting to process personal data and information to be provided upon request of data subject); Identity theft (both online and off-line).

Inspection Activities	
Inspections, investigations	677 (only ~ 5 % are self-initiatives)
Sanction Activities	
Sanctions	Administrative sanctions applied in 36 cases – 14 warnings and 22 penalties.
Penalties	20 476 55 LVL (29 135,50 EUR).
DPOs	
Figures on DPOs	42 DPOs assigned by the controllers

B. Information on case-law

No specific achievements.

C. Other important information

In order to foster mutual cooperation, the Data State Inspectorate of Latvia participated in the annual meeting of the three Baltic States where a decision was made to perform an annual joint inspection of personal data protection in SPA's and recreational facilities in 2014. An Annual joint inspection on gambling establishments and casinos concluded in 2013.

LITHUANIA



A: Summary of activities and news

As Lithuania held the presidency of the Council of the European Union from 1st July to 31st December 2013, the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – the SDPI) focused their attention on data protection reform, and actively participated in the meetings of the working group DAPIX.

European Data Protection Day was celebrated on 25th January 2013. A press conference at the Seimas of the Republic of Lithuania on Data Protection Day known as “Data protection in the European Union and Lithuania” was organised. In addition, Data Protection Day was commemorated at Mykolas’s Biržiška High school on 4th February 2013. The SDPI organized a seminar for the students of this high school about privacy and publicity in an information society, passports of the Republic of Lithuania, social networks, and similar problems.

The SDPI actively participated in the conference “Personal Data Protection: use for a person and business”, that was organised by the Business Confederation of Lithuania on 9th May 2013.

The Latvian, Lithuanian, and Estonian data protection supervisory authorities met with the aim of continuing Baltic States cooperation in March 2013 in Ryga, Latvia. The Personal Data Supervision Authorities of the Baltic countries carried out a joint investigation regarding personal data processing and protection within the gambling sector for a second time. In total, 13 casinos in the Baltic countries were inspected in 2013.

The Information system “HELP” was launched in 2013, implementing access to the SDPI via electronic communications networks. Consequently, data subjects and data controllers have the possibility to lodge complaints or any other application to the SDPI electronically in any place at any time and will receive a reply in the same manner. Now data subjects and data controllers have the possibility of seeing who is dealing with their case, what the procedure is, and what stage the case is at.

Dr. Algirdas Kunčinas was appointed to the position of the director of the SDPI for a second term of office of five years. The new term of office started from the 1st of January 2014.

Organisation	
Chair and/or College	Dr. Algirdas Kunčinas
Budget	1 919 000 Litas (555 781 euros)
Staff	30
General Activity	
Opinions, recommendations	N/A
Notifications	1 409
Prior checks	338
Requests from citizens	23
Complaints from citizens	327

Advice requested by parliament or government	N/A
Other relevant general activity information	3 845 consultations; 100 public information releases; 4 summaries on the preventive investigations results and case law; 29 conclusions on the EU and the Council of Europe documents; 65 responses to inquiries from parties of Convention (ETS No. 108); 309 coordinated legal acts and data controller documents; 11 prepared legal acts, 6 public consultations.
Inspection activities	
Inspections	51
Sanction activities	
Sanctions	The SDPI drew up 41 protocols of administrative offences
Penalties	N/A
DPOs	
Figures on DPOs	N/A.

B. Information on case law

Processing of personal identification number

A person lodged a complaint because a company providing internet and cable television services asked the complainant to sign a standard contract and to write his personal identification number in the contract. According to paragraph 2 of Article 7 of the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter, the LLPPD) it shall be permitted to use a personal identification number when processing personal data only with the consent of the data subject. Paragraph 3 of this Article determines exceptions to this rule. The SDPI stated that the consent of the complainant was not free because otherwise he would not get the service and gave a legally binding instruction to the company to change the form of the standard contract and not to require the personal identification numbers of their customers. This instruction was appealed to the Vilnius District Administrative Court by the complainant. The Court dismissed the appeal as unfounded, concluding that the decision of the SDPI that the consent of the complainant had not been freely given was correct. The complainant appealed this decision to the Supreme Administrative Court, which also stated that the instruction of the SDPI had been correct and the arguments of the company that the personal identification number is necessary in the contract are not important in this case.

Disclosure of personal data to media

A person lodged a complaint because the State Tax Inspectorate disclosed his personal data about a tax inspection that was still in process to media. According to paragraph 1 of Article 38 of the Law on Tax Administration of the Republic of Lithuania, the tax administrator shall keep Information on tax payers confidential and use it only for lawful purposes. According to subparagraph 6 of paragraph 2 of Article 38 of this law information related to tax violations shall not be kept confidential if the taxpayer's fault for tax law violations is proven. The SDPI decided that the State Tax Inspectorate disclosed personal data of the complainant about the tax inspection that was started but was not completed at that time

yet illegally, not having any legal ground provided for in Article 5 of the LLPPD or any other criteria for lawful disclosure of personal data. The SDPI gave an instruction to the State Tax Inspectorate not to use the former practice to inform media (according to requests of the media) about tax inspections of natural persons while they are still in process because the taxpayer's fault for tax law violations has yet to be proven.

This instruction was appealed to the Vilnius District Administrative Court by the State Tax Inspectorate, who plead that disclosing the facts of a tax inspection that has started is one of the means of preventing violations and giving information about the activity of the institution. The Court dismissed the appeal, based on Article 38 of the Law on Tax Administration, and stated that disclosure of a taxpayer's personal data could not be justified with the aim of preventing violations and providing information about the activity of the institution.

The State Tax Inspectorate appealed this decision to the Supreme Administrative Court, which also dismissed the appeal.



LUXEMBOURG

A. Summary of activities and news

Legislative changes

There were no legislative changes in the field of data protection and privacy in 2013.

Key topics

One of the missions of the CNPD is to advise the Luxembourgish government on topics in relation to privacy and data protection. 10 formal opinions on laws and regulations were issued in 2013. The main topics were:

- the organization of the national intelligence service;
- the status, the designation procedure, and the powers of the coordinating doctor (*“médecin coordinateur”*);
- the reform of the law concerning the public service;
- the reform on the execution of the sentence and the penitentiary administration;
- the cross-border exchange of information on road safety related traffic offences;
- the national cancer register.

In the field of smart metering, the CNPD is assisting Luxmetering with the implementation of their operating processes and procedures as part of a Privacy Impact Assessment (PIA). Luxmetering is an economic interest group (*“Groupement d'intérêts économique”*) composed of 7 Luxembourgish electricity and gas network operators. It is responsible for the implementation of the infrastructure and the national deployment of approximately 350,000 smart meters.

News

The CNPD and the CNIL (France) performed a review of the “Microsoft Services Agreement” and the “Microsoft Online Privacy Statement” at the request of the Article 29 Working Party after the company changed its contractual terms of use. Previous examples, where companies like Google or Facebook modified their terms of use, have shown that these changes can have wide-ranging effects in Europe and could potentially weaken the protection of personal data and privacy of individuals.

After the revelations in the international press concerning the PRISM-Program, the Luxembourgish DPA received two requests from European citizens to verify if Skype and Microsoft Luxembourg had processed their data lawfully and if the companies had shared their data with the US National Security Agency.

As the lead DPA, the CNPD approved the BCRs of the Luxembourg-based multinational steel group ArcelorMittal after 18 months of discussions, together with the DPAs of the 25 other European countries in which the ArcelorMittal group is present. This was the second BCR approval procedure for the CNPD, which also acted as lead DPA for eBay's BCRs in 2009.

Key events and awareness raising

To celebrate its 10 year anniversary, the CNPD organized a conference on 28th January 2013 (Data protection day) with Dean Spielmann (President of the European Court of Human Rights) on the topic *"Data Protection in the case law of the European Court of Human Rights"*.

In addition to this big event, the Luxembourgish DPA participated in multiple awareness-raising events aimed at the general public as well as in awareness-raising seminars and training courses among a more specialised public. One example where the CNPD participated was a conference for the Data Protection Officers organized by the AFCDP (*Association Française des Correspondants à la Protection des Données à caractère Personnel*) in Luxembourg.

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	1 552 000 €
Staff	College: 3 Legal department: 5 Notifications and Prior checks: 2 General administration: 2 Communication and documentation: 1 IT and logistics: 1 Total: 14
General Activity	
Decisions, opinions, recommendations	693
Notifications	1 072
Prior checks	725
Requests from data subjects	270
Complaints from data subjects	177
Advice requested by parliament or government	10
Other relevant general activity information	Meetings and consultations (w. public/private sector): 177 Information briefings and conferences: 18

Inspection Activities	
Inspections, investigations	26
Sanction Activities	
Sanctions	1
Penalties	N/A
DPOs	
Figures on DPOs	Designated DPO's during 2012: 20 Total of designated DPO's (at date of report): 49

B. Information on case-law

Court of First Instance, Labour chamber, 7 March 2013, on the validity of proof (e-mail correspondence) collected in absence of a prior authorisation by the CNPD

The main question of this case pertained to the determination as to whether the dismissal with immediate effect of an employee of company X was to be considered excessive or justified. The employer invoked unfair competition practices by the employee and introduced as proof, among others, a list of e-mails written and sent by the employee. The employee demanded that these specific supporting documents had to be removed from the proceedings, as no prior authorisation from the CNPD had been obtained. (N.B.: under Luxembourgish law, the surveillance of employee's e-mail correspondence is subject to a prior authorisation to be obtained from the CNPD).

After establishing that no prior authorisation had been given in this case and invoking the fundamental rights of the secret of correspondence, as well as the right to privacy, the Court of First Instance held that said documents had to be removed from the proceedings.

This decision is very interesting in the sense that the Court of First Instance, in the domain of e-mail surveillance, took the exact opposite stance as the majority of cases in the domain of video-surveillance, where most decisions state that images can be admitted as proof, even in absence of a prior authorisation by the CNPD. It must be noted however that this is only the first instance court and that Company X may have appealed. No decision has however been published as of the day of this writing.

C. Other important information

In 2013, the first association on privacy and data protection was established in Luxembourg. The members of the APDL (*Association pour la protection des données au Luxembourg*) are mainly Data Protection Officers, IT security experts, and compliance officers, as well as lawyers and consultants.



MALTA

A: Summary of activities and news

During 2013, the Office of the Information and Data Protection Commissioner maintained a proactive approach to meet the sectors with the firm objective of discussing their business operations and addressing any arising data protection issues which would require an intervention by the Commissioner. This Office adopts an approach to coordinate such meetings with the wide representation of the respective sector. This approach proved to deliver satisfactory results, particularly where guidelines or codes of practice would need to be developed to regulate specific areas of the sector.

Although no legislative intervention was made to the Data Protection Act or to the subsidiary legislation issued thereunder, during the year this Office carried out internal review exercises designed to implement the Government's overarching policy to ensure better regulation.

In March, voters were called to the polls to cast their preference in the general election. During the electoral campaign period, this Office experienced a significant increase in the number of complaints received. The majority were submitted by data subjects who contended a breach of their data protection rights by political parties or election candidates when the latter sent political campaigning messages by means of electronic mail or SMS. The complaints were lodged by individuals who were neither enrolled as members of any party nor had given their prior consent to receive these types of unsolicited messages.

To address this situation, immediately following the election, the Commissioner requested a meeting with the main political parties to inform them that the time was ripe for development of a set of guidelines concerning the processing of personal data for political campaigning purposes. The purpose of these guidelines is to provide a clear and uniform interpretation of the applicability of the Data Protection Act in a political environment where political parties and candidates process personal data about individuals for the purposes of carrying out political campaigns and promoting their political ideology. Following a series of meetings and written contributions received from the parties involved, this Office prepared a final draft to be agreed upon and, in terms of established timelines, will be adopted in the third quarter of 2014.

During the period under review, the Office continued to honour European and international commitments by participating in various data protection forums. On the 28th of January, similar to previous years, this Office prepared informative material and stationery items which were distributed to students, in pre-determined grades, where the concept and the inherent message was safety on the internet.

In regard to the implementation of the Freedom of Information law, during 2013, Public Authorities gained experience in the implementation of the Act and the processing of requests for documentation through the use of the dedicated IT system. Intervention and support delivered by the Freedom of Information Coordinating Unit, established within this Office's line Ministry, were instrumental in assisting Public Authorities in achieving these aims.

Public Authorities dealt with a total of 130 requests for information, 10 of which were brought forward from 2012. Out of this total, 71 (54.6 %) were accepted while 51 (39.2 %) were rejected. The number of requests still pending a decision at the end of the year was 4 (3.1 %). Another 4 requests (3.1 %) were abandoned by the applicants. Out of the rejected cases, 14 (27.4 %) addressed a request to the Commissioner for a review of the decision. The Commissioner decided in favour of the applicant in one case and rejected the other 13. Out of these 13 cases, 3 submitted an appeal to the Information and Data Protection Appeals Tribunal. A fourth person also felt aggrieved by a decision of the Commissioner in relation to a data protection complaint and lodged an appeal before the Tribunal.

By the end of the year all these appeals were still awaiting judgement pending the appointment of the Tribunal whose members tendered their resignation following the change in the State's administration.

Organisation	Office of the Information and Data Protection Commissioner
Chair and/or College	Information and Data Protection Commissioner
Budget	ca. €280 000
Staff	Commissioner – 1 Professional staff – 3 Technical Support- 2 Administrative Support – 3
General Activity	
Decisions, opinions, recommendations	81 decisions were issued by the Commissioner for both data protection and freedom of information. 28 Opinions/Recommendations concerning specific data protection matters were issued by the Commissioner and addressed to data controllers.
Notifications	240 new notification forms
Prior checks	6 prior checking requests were received
Requests from data subjects	Queries received by phone were an average of 10 calls daily whereas queries received by email amounted to ca. 250 requests
Complaints from data subjects	144 complaints on Data Protection matters and 14 on Freedom of Information.
Advice requested by parliament or government	1 request was received from the Ministry for Education and Employment related to the drafting of a legal instrument requesting personal data on students for the purpose of developing target policies to address the growing problem of low achievers in schools.
Other relevant general activity information	n/a
Inspection Activities	
Inspections, investigations	10 on-the-spot inspections were carried out mainly as part of the complaints investigation procedure.
Sanction Activities	
Sanctions	Official admonishments were issued to data controllers but no legal proceedings were initiated before the Courts of Law.

Penalties	1 financial penalty was imposed on a data controller following a repeated offence which was established after the conclusion of an investigation.
DPOs	
Figures on DPOs	14 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, media reports, etc. In 2011, a new signal registration system was introduced that enables the Dutch DPA 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 2013 were, among others, profiling, adequate protection of medical data, and data processing in the employment relationship. In addition, the activities undertaken by the Dutch DPA in 2013 focused on the legal principles of purpose limitation, consent, transparency, and data security in particular.

One of the major investigations carried out in 2013 focused on the protection of medical data. Everyone has the right to the same level of protection against unauthorized access to his or her medical data. However, an investigation conducted by the Dutch DPA at different health care facilities, after-hours clinics, and pharmacists showed that there are many problems with the security measures taken to protect patient data against such unauthorized access. Insufficient security measures risk medical files being accessed by employees who are not in any way involved in the treatment of the patient. The Dutch DPA considers that, based on the investigations, the signals received, and conversations with the branch-organisations, the problems detected appear to be relatively common in the health care sector.

The transfer of patient data by one health care provider to another, for example by a doctor's office to an insurance company or pharmaceutical company, is subject to very strict safeguards. These transfers are not allowed without the consent of the data subject. The Dutch DPA investigated the transfer of medical data by pharmacists to a company producing materials for people with incontinence and concluded that the pharmacists had not taken enough safeguards to protect the patient data. Furthermore, not all patients had given their consent to the transfer of their data to the pharmaceutical company.

Another set of investigations carried out in 2013 dealt with online data and profiling. Data on television programmes watched, websites visited, and apps downloaded say a lot about an individual's behaviour and preferences, but it is often not clear what happens to this data collected by telecom providers and app developers. Most people are not aware that for these so-called 'free' services, they are actually paying with their personal data. Companies and organisations have to provide sufficient information to individuals in regard to the use of their data and have to ask for their consent where necessary.

One of the investigations in this area conducted in 2013, was an investigation regarding illegitimate data-analyses (packet inspections) undertaken by four telecom providers. These companies were found to store data regarding which websites and apps were visited by the customer in violation of the law and, in addition, did not correctly inform the customer thereof.

Furthermore, parliamentary questions regarding the use of cookies by the Dutch Public Television Broadcaster (Nederlandse Publieke Omroep – NPO) on their websites, caused the Dutch DPA to issue further guidance on the legal framework in this regard, stating that NPO was not allowed to refuse visitors access to their website if they did not consent to the tracking of their browsing behaviour.

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 2013, advice was given on the draft Youth Act (Jeugdwet). The draft Youth Act deals with the delegation of tasks, both administrative as well as financial, from the national government to the municipalities with regard to providing assistance, help, and care concerning the upbringing of children and youths with psychological problems. The exact division of tasks is not yet fully clear, but the Dutch DPA expects that decentralisation, a trend which it has more often detected in other proposed legislation, will lead to an increase in the amount of data that is to be processed by municipalities. The comprehensive approach to youth- and family problems is furthermore expected to lead to an increase in the exchange of information between the different stakeholders, also increasing the risks of excessive data processing operations, of (unlawfully) using data for another (non-compatible) purpose, and of insufficient security measures.

From public information available on the decentralisation of the youth care system, it seems that municipalities and other involved parties do not take measures to mitigate these risks. The draft law furthermore does not appear to be providing the necessary resources to build a system ensuring the careful and legitimate processing of data. The Dutch DPA is therefore of the opinion that municipalities should be obliged to carry out Privacy Impact Assessments and audits with regard to (current and proposed) data processing operations. This should be provided for in the proposed Youth Act or in secondary legislation.

Organisation	Dutch Data Protection Authority
Chair and/or College	Jacob Kohnstamm – Chair Wilbert Tomesen – Commissioner and Vice-Chair Madeleine McLaggan-Van Roon – Commissioner* <i>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 the request of the Secretary of State for Security and Justice.</i>
Budget	Allocated: €7 586 000- Executed: €7 827 000-
Staff	74.9 FTE
General Activity	
Decisions, opinions, recommendations	109 (guidelines, opinions, codes of conduct, international cases, exemptions, sanctions, and international transfers)
Notifications	3 523
Prior checks	86

Signals ⁽⁶⁾ from data subjects	6 879
Advice requested by parliament or government	30
Other relevant general activity information	n/a
Inspection Activities	
Inspections, investigations	73
Sanction Activities	
Sanctions	19
Penalties	n/a
DPOs	
Figures on DPOs	369 (in 362 organisations)

B. Information on case-law

During the year of this report, several data protection related cases have been dealt with by the courts in the Netherlands. One of the cases concerned a complainant who requested to the National Forensic Institute (NFI) if she could use a drop of blood from a deceased person, that the NFI held in one of its filing systems, in order to determine whether they were family. Following objections by the daughters of the deceased, she was denied the use of the drop of blood. She appealed this decision at the Public Prosecutor's Office and the NFI, to which the Public Prosecutor replied that the decision not to allow her to use the blood could not be seen as a decision having legal effects, based on the Judicial Data and Criminal Records Act, and her appeal was therefore inadmissible.

She appealed at the Court of Rotterdam, who reviewed whether the decision was indeed a decision not having legal effects, based on the Judicial Data and Criminal Records Act. The Court came to the conclusion that it was not the Judicial Data and Criminal Records Act, nor the Undertaking Act, that was applicable in this situation. Considering it concerned bodily material, the Dutch Data Protection Act was applicable. The woman should therefore have gone to a civil court and appealed on the basis of the Data Protection Act, instead of appealing to the Public Prosecutor and the NFI in an administrative procedure.

In another case in 2013, a complainant appealed to the Supreme Administrative Court that he was, unrightfully, not given the right to access, rectify, or delete information in a file held on him by the Dutch Immigration and Naturalisation Service (IND).

The complainant was in possession of a residence permit on the basis of the fact that he was married to person X. The Minister of Justice then received an anonymous letter stating that the complainant was not the spouse of person X, but that they were brother and sister instead. He therefore sent a letter to the complainant stating that, following information received anonymously, the Minister had the intention

⁶ Since April 2011, all citizen contacts are registered as a signal. These signals are used to prioritise our tasks. Therefore, it is not the means by which signals are received by the DPA that are measured, but the sector to which they are subjected.

of repealing the residence permit of the complainant and offered the possibility of voluntarily cooperation to perform a DNA test to establish the facts. The complainant refused to take the DNA test. This made it technically impossible to determine whether the anonymous letter was stating the facts and caused the Minister to decide not to repeal the residence permit.

The complainant subsequently wanted to sue the writer of the anonymous letter for libel and defamation and asked for access to this document in his file in order to rectify or delete it. He felt that, since it contained personal information about him, he should be granted access to and be allowed to delete the letter. The Minister refused to give him access on the basis that it was necessary to protect another individual and the rights and freedoms of others. Besides, he was given a factual overview of the content of the letter. The Court confirmed and furthermore stated that the content of the letter did not concern personal data of the complainant. The complainant appealed to the Supreme Administrative Court on the basis of Article 8 of the European Convention on Human Rights (ECHR).

The Supreme Administrative Court ruled that the right to correction in the Dutch Data Protection Act is not meant to rectify or delete information that is not to the liking of the complainant. Whether the information in the concerned letter is correct or not should be assessed in an appropriate procedure. Such a procedure, the investigation with regard to the residence permit of the complainant, was conducted. The fact that the outcome of the investigation was that it was technically not possible to establish the facts, does not influence the fact that the Minister deems the letter relevant and that he was right in keeping the letter, after having weighed his interests against those of the complainant's interests in deleting the letter. It furthermore ruled that the protection of the plaintiff was correctly deemed more important than the interests of the complainant. The decision to not delete the letter was therefore, insofar as it would have been a violation of his rights under article 8 ECHR, permitted by the Dutch Data Protection Act, following paragraph 2 of article 8 of the ECHR.

POLAND



A. Summary of activities and news

As of 22 March 2013, the Inspector General for Personal Data Protection (GIODO) became a competent authority to accept personal data breach notifications made by providers of publicly available telecommunications services. This new obligation is a consequence of the amendment of the Act Telecommunications Law, which implements into Polish law the provisions of Directive 2002/58/EC on privacy and electronic communications introduced by Directive 2009/136/EC from 25 November 2009 amending the Directive on universal service (2002/58/EC) – or the so-called Citizen’s Rights Directive.

As regards the above obligation, a relevant electronic form was developed to report data protection breaches and a Data Breach Team was set up to analyse data breaches, which includes assessing the adequacy of remedies introduced by operators in connection with reported breaches.

In 2013, GIODO received 139 data breach notifications from telecommunications operators.

In 2013, GIODO regularly modified and improved electronic communications means with data controllers and citizens. Activities were also undertaken related to migration of applied IT technologies from client-server architecture to technology using private cloud architecture.

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

1. On 1 March 2013, a meeting of the Inspector General with Françoise Le Bail, Director General of the European Commission’s DG Justice was held. The meeting was devoted to the analysis of the EU data protection framework reform’s progress and touched upon issues which raise the biggest controversies in the ongoing debate or are of significant importance for the future shape of the provisions on personal data protection in Europe.
2. On 16 April 2013, a joint meeting of the Senate Committees was organised in the Senate (upper chamber of the Polish Parliament) in cooperation with GIODO. During the debate, the main directions of changes of the UE data protection framework, impact of the General Regulation on the situation of Polish entrepreneurs and consumers, and its relation to the national provisions in the light of challenges of globalisation and contemporary business models were discussed.
3. On 4 April 2013, GIODO, as well as representatives of the EC, the Permanent Representation of the Republic of Poland to the EU, MEPs, representatives of ministries, NGOs, business, academics and independent experts participated in a discussion on data protection reform organised by the Ministry of Administration and Digitisation which is a leading authority on the works on the General Regulation in Poland. A similar meeting devoted to the reform was held on 13 May 2013 as part of the debate “Digital identity: Who are we online and how do we share knowledge on ourselves?”. Commissioner Viviane Reding, Vice-President of the European Commission, leading the works on the proposal of the new Regulation of the European Parliament and of the Council of the European Union, was a special guest at the latter meeting.

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	135 employees.
General Activity	
Decisions, opinions, recommendations	<p>1 358 decisions issued (504 decisions related to registration proceedings, 74 were issued in connection with conducted inspections, 646 were issued as a result of proceedings initiated by a complaint, 134 concerned authorisation to data transfer to a third country, and 109 related to administrative execution).</p> <p>121 addresses and requests were addressed to state authorities, territorial self-government authorities, as well as to state and municipal organizational units, private entities performing public tasks, natural and legal persons, organizational units without legal personality, and other entities in order to ensure efficient protection of personal data</p>
Notifications	16 866 personal data filing systems registered.
Prior checks	As a result of registration procedures (prior checking) 2 279 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.
Requests from data subjects	<p>4 911 legal questions were sent to the Polish DPA.</p> <p>11 908 explanations were also provided through GIODO's information hotline.</p>
Complaints from data subjects	<p>Complaints concerning infringement on personal data protection, including</p> <ul style="list-style-type: none"> - public administration (126 complaints), - courts, public prosecutor's office, the Police, bailiffs (56 complaints), - banks and other financial institutions (127 complaints), - Internet (124 complaints), - marketing (31 complaints), - housing related (57 complaints), - social, property, and personal insurance (50 complaints), - social organisations (12 complaints),

	<ul style="list-style-type: none"> - telecommunications (24 complaints), - employment (11 complaints), - debt collection (42 complaints), - education (21 complaints), - health care (34 complaints) - other (386 complaints).
Advice requested by parliament or government	Opinions were expressed on 617 draft acts submitted for review to GIODO.
Other relevant general activity information	<p>60 - number of training courses conducted by GIODO concerning provisions on personal data protection, especially for public institutions.</p> <p>209 education establishments, including primary, middle, and secondary schools, and teacher vocational training centres, participate in the 4th edition of the Poland-wide programme “Your data, your concern. Educational initiative addressed to students and teachers” for the academic year 2013/2014.</p>
Inspection Activities	
Inspections, investigations	<p>173 inspections were conducted in 2013.</p> <p>Sectoral inspections related to:</p> <ul style="list-style-type: none"> - online services (including online shops) – 10 inspections, - entities executing loyalty programmes – 7 inspections, - mega stores using RFID – 8 inspections - territorial self-government authorities collecting data for the purposes of garbage disposal (in connection with execution of the Tidiness and Order Act) – 15 inspections, - police units using “e-posterunek” (e-police station) electronic system (facilitating the work of the Police) – 8 inspections, - authorities authorised to process data in the National Information System and the Visa Information System – 14 inspections, - telecommunications services providers (in connection with data breach incidents) – 14 inspections.
Sanction Activities	
Sanctions	<p>GIODO keeps no general statistics on sanctions.</p> <p>However, for example in connection with GIODO’s powers of an enforcement authority, 109 administrative proceedings were instituted within execution of GIODO’s decisions.</p> <p>Whereas in connection with inspections conducted in 2013, GIODO instituted administrative proceedings against data controllers and</p>

	<p>issued 74 administrative decisions which included an order to restore a proper legal state.</p> <p>Also, GIODO issued 92 decisions on refusal to register a data filing system.</p> <p>No sanctions imposed by the DPA in the reporting period.</p>
Penalties	No fines were imposed in 2013.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In 2013, 52 out of 646 administrative decisions issued by GIODO were appealed against before the Voivodeship Administrative Court in Warsaw. In comparison, in 2012 70 decisions were appealed against, indicating decrease of 18.

Among the judgments issued as a result of entities' complaints against the DPA's decisions, the judgment by the Supreme Administrative Court on 21 August 2013 (ref. no. I OSK 166/12) is especially noteworthy. In this judgment the Court indicated that the wording of Art. 18 (6) of the Act on providing services by electronic only indicates the obligation to provide information on data to state authorities for the purposes of conducted proceedings; whereas no ban results disclose those data to persons whose rights have been infringed. Both the authority ordering the disclosure of data and the administrative court considering the complaint against such a decision each time have to, considering the individual circumstances of a given case, balance the opposite interests, i.e. the right to personal data protection and the right to dignity, reputation, or a company's image. In doing this, the requirements resulting from the proportionality principle have to be properly taken into account, so that the applied measures are adequate to the risk for the interest requiring more protection in a specific case. The Supreme Administrative Court emphasised that the current legal circumstances allow for the conclusion that, that under the current law, one can demand the disclosure of data collected by the controller of the online service by using a less restrictive act than the Act on providing services by electronic means, that is the Act on Personal Data Protection, and specifically its Art. 23 (by data processing, including their disclosure), but subject to certain conditions. The latter include the proportionality of means and purposes as well as balance of protection of different interests: freedom of expression and the right to the protection of personal interests. The entity demanding the disclosure of personal data has to justify its standpoint. Pursuant to Art. 23 (1) (5) these must be "legitimate interests". In case of refusal to disclose the data by the entity, being their controller, the party may submit a request to GIODO, which after having conducted relevant proceedings can by way of a decision order the disclosure of personal data. In this regard, GIODO's evaluation is significant and should depend on the circumstances of a given case, because both the Act on providing services by electronic means and the Act on Personal Data Protection will apply in this respect. While making a decision, GIODO has to assess in each individual case, and which interests protected by the law are more important – personal data or the company's economic interests.

In 2013, the Supreme Administrative Court dismissed a last resort appeal of the W. Commune Head against the Voivodeship Administrative Court's judgment on 24 November 2011 (ref. no. II SA/Wa 1828/11). In the judgment on 14 March 2013 (ref. no. I OSK 620/12), the Supreme Administrative Court indicated the rightness of decisions issued by GIODO in its administrative proceedings. The Supreme Administrative Court emphasised in the above mentioned judgment that: "While examining the legitimacy of personal data processing (...) both GIODO and the Court of First Instance properly used the principles specifying admissibility of the processing of personal data provided for in Art. 23(1) of the Act

assuming that the prerequisite legitimising the processing of those data was the one enumerated in point 2 of the above provision. The latter allows for the processing of personal data, if it is necessary for the purpose of exercise of rights and duties resulting from a legal provision. In this case, the obligation resulting from a legal provision was placed by the Commune Head of the information in regard to the contents of the resolution by the Commune Council in the official online publication – Public Information Bulletin (BIP). To fulfil this obligation, it was not necessary to disclose the data of a natural person who submitted a complaint against the Commune Head's activity. If the purpose of placing public information in the BIP is transparency of public activity of the Commune Council, including the contents of its resolutions, then this purpose is also achieved when the data on private persons are erased from the information to protect privacy.

C. Other important information

In the reporting period, growth in the number of files notified to registration (**when compared to 2012 by 40 %, to 2011 – by 81 %, and to 2010 – by as much as 242 %**) was observed. Moreover, it needs to be noted that more and more notifications come from private entities – in 2013, the number of notifications from those entities increased by 95 % when compared to 2012, whereas the number of notifications by public entities in this period increased by 3 %. In consequence, during the reporting period as much as 46 % of the overall number of notified files came from private entities, while in both 2012 and 2011 the rate amounted to 31-32 %. In 2013, GIODO handled **3 709** updating notifications submitted by data controllers, whereby GIODO issued 340 decisions on removal of a data filing system from the Poland-wide open register of personal data filing systems.

On European Data Protection Day on 28 January 2013, the Inspector General has traditionally organised an Open Day for all citizens, and a Conference entitled "Personal Data Protection in Health Care and Clinical Trials". Also, as usual, European Data Protection Day was celebrated in Brussels. Moreover, GIODO took an active part in the 5th International Conference on Computers, Privacy and Data Protection (23-25 Jan.), within the framework of which, on 23 January 2013 a special panel was organised by the Polish DPA devoted to the legislation in Poland entitled "*From 'Solidarity' to the Surveillance Society. Privacy Protection Dilemmas in Poland*".

GIODO continued its initiative consisting of organising additional open days in other cities all around Poland and organised the 3rd Open Day on 6-7 May 2013 in Poznań, which included, among others, a scientific conference devoted to the legal and economic aspects of personal data processing for economic purposes, as well as a series of meetings in the form of seminars and training courses for public administration.

On 23-26 September 2013, GIODO hosted the 35th International Conference of Data Protection and Privacy Commissioners "Privacy: A Compass in Turbulent World" in Warsaw, Poland. The conference contributed to a better understanding of data protection issues around the world and, furthermore, set the grounds for exchanging experiences and views in this field. It also provided a better explanation of the problems related to data protection. During the Closed Session of the 35th International Conference, we hosted 66 delegations from all over the world. Thus, the experience and knowledge of so many participants provided a unique possibility to adopt as many as 8 [resolutions](#) concerning different areas of data protection, i.e. resolutions on accreditation, profiling, the Conference's strategic direction, international enforcement coordination, openness regarding personal data practices, digital education for all and web-tracking and privacy. Moreover, the "Warsaw Declaration on the "appification" of society" was adopted. The Open Conference gathered representatives from many milieus, including politics, science, business, national and international NGOs, who debated in groups divided into three themes: "Reforms all over the world. Interoperability between the regions", "Privacy and Technology", and "Actors: perspectives, roles, interests". During the Open Conference the "Warsaw Declaration 2013: Call for incentives to promote the appointment of DPOs" was adopted by the Confederation of European Data Protection Organisations and the National DPO Associations in Europe.

In 2013, the **PHAEDRA project** (Improving practical and helpful cooperation between data protection authorities) co-funded by the European Commission under the programme Fundamental Rights and Citizenship "Action grants" was launched. GLODO participates in the project as a member of the project consortium. The project is realised in cooperation with Vrije Universiteit Brussel (project coordinator), UK Trilateral Research & Consulting LLP (partner), and Spanish Universitat Jaume I (partner). The basic objective of the project is to identify the problems hampering cooperation between particular data protection authorities and other state entities dealing with this issue as well as to draw up recommendations aimed at improving the situation. As a result, the project will contribute to improve co-operation and co-ordination between all stakeholders. The project is to be finalised in 2015.

PORTUGAL



A. Summary of activities and news

In May 2013, the Portuguese DPA hosted the Data Protection Spring Conference, which convened in Lisbon with approximately 130 participants to discuss *Protecting Privacy: the challenges ahead*. Right in the middle of the EU data protection reform and during the modernisation of Convention 108, the European Commissioners Conference discussed important issues for the future of data protection, such as the concept of personal data, the rights of the data subjects on the Internet, information security as a priority, the strengthening of supervision, and cooperation.

The PT DPA signed a cooperation protocol with the research centre of the Faculty of Law of the University of Lisbon to jointly raise awareness on data protection and privacy issues and to support each other on relevant initiatives.

The DPA issued new guidance on the control of the use of ICT in an employment context, reviewing its 2002 Guidelines, bringing into consideration new labour legislation and new developments in this area, so there was a need to update and better detail some aspects of the private use of ICT by employees http://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf

The DPA also followed up the development of the e-health records project, by authorising phase II of the health records platform (PDS), setting important conditions for personal data processing, and including the implementation of Privacy by Design tools, to enhance the privacy of citizens while providing them with control in regard to the access and use of their data.

Following the practical implementation of the e-Privacy Directive update, the Portuguese DPA had important meetings with representatives of the economic stakeholders in the field of e-commerce and marketing to discuss the new legal framework, regarding cookies in particular.

As for the e-notification, the DPA developed more specific notification forms, for particular cases, for data processing by video surveillance, in this way increasing the number of full electronic proceedings.

Organisation	CNPD – Comissão Nacional de Protecção de Dados
Chair and/or College	Prof. Dr. Filipa Calvão (President)
Budget	2 356 436 Euros
Staff	From 25 to 18 (by the end of the year) due to legal restrictions imposed on the public service
General Activity	
Decisions, opinions, recommendations	12 285
Notifications	11 170
Prior checks	10 280
Requests from data subjects	89 requests regarding access and deletion to the Schengen Information System

Complaints from data subjects	652
Advice requested by parliament or government	88
Other relevant general activity information	259 requests to access personal data by third parties 910 requests for opinions on lifting the caller's confidentiality because of troubling phone calls 2 585 information requests (from data controllers and data subjects) submitted in writing via website to the Front Office
Inspection Activities	
Inspections, investigations	246
Sanction Activities	
Sanctions	158
Penalties	± 205 000 Euros
DPOs	
Figures on DPOs	Not applicable

ROMANIA



A. Summary of activities and news

Organisation	National Supervisory Authority For Personal Data Processing
Chair and/or College	Ancuta Gianina Opre
Budget	3 460 000 RON (approx. 772 321 EUR)
Staff	43 plus the President and the Vice-president of the authority
General Activity	
Decisions, opinions, recommendations	632 out of which 5 decisions for the deletion of personal data were processed, 1 decision for ending the data processing and for the deletion of the personal data processed, and 1 recommendation
Notifications	7 499
Prior checks	-
Requests from data subjects	156
Complaints from data subjects	721
Advice requested by parliament or government	32
Other relevant general activity information	-
Inspection Activities	
Inspections, investigations	229 in situ and 44 in writing
Sanction Activities	
Sanctions	66 fines with a total amount of 134 500 RON (approx. 30 022 EUR)
Penalties	124 warnings
DPOs	
Figures on DPOs	-

B. Information on case-law

Case-law 1

A court disclosed the personal data of a victim of a criminal offence, without his/her consent, in a press release issued by its spokesperson.

The press statement was broadcast at the same time by a TV network on its news programme, with the video recording of the statement being posted on the website of that respective television from which it could be accessed by any visitor of the website.

The representative of the controller stated that when giving the interview, the spokesperson quoted from a document drafted according to the state of fact and where the name and surname of the victim appeared. In the press release issued further, the identification data of the victim were anonymised using the initials of the name and surname.

The controller was sanctioned for the contravention foreseen by Article 32 of Law no. 677/2001.

At the same time, it was recommended that the controller create a document to prove the training of its spokespersons concerning the data protection of the data subject in relation to mass-media.

Case-law 2

A petitioner claimed to have received repeatedly unsolicited commercial communications from a travel agency whose services he/she claimed he/she never used. The petitioner also referred to the fact that the commercial messages did not contain the full contact details of the travel agency that continued to send him/her commercial messages even after he/she used the unsubscribe mechanism from the content of the messages asking not to receive such messages.

Following the verification of the commercial messages received by the petitioner, it was found that they did not indicate the exact name of a commercial company. The data protection authority carried out several investigations both in writing and to the headquarters available for that company. It was able to ascertain the refusal of the representatives of the travel agency to provide information requested by the data protection authority in exercising its investigation powers, as well as the continued transmission of commercial communication to the petitioner despite the opposition shown by him/her repeatedly.

Taking into account the findings, the controller was sanctioned based on Law no. 677/2001 and Law no. 506/2004 because the company refused to provide the information and to participate in the announced investigation, continued to send repeated commercial communication to the petitioner even though he/she did not give his/her expressed consent for receiving such commercial communication. In addition, most of the messages did not contain the full contact details concerning the real identity of the sender.

Case-law 3

The Ministry of Internal Affairs informed the data protection authority with reference to the disclosure of several categories of personal data on the Internet and sent, as proof, an optic device on which documents containing personal data were stored.

Through this notice, the data protection authority was informed of Internet (an ODC network) documents representing different notary acts: addresses to different notary offices, to central/local public authorities, contracts, mandates, declarations of natural persons, declarations of certain magistrates of parquet referring to their non-cooperation with intelligence services or their non-membership to the political police, authentication documents, etc.

Following the investigation carried out, the public notary from which those documents originated admitted that the documents were real, being written on the computer of his/her employees but he/she could not explain how they became public on the Internet. According to the declaration of the notary, there were some problems concerning the malfunction of those computers following a virus on their computer.

At the date of the investigation, it was found that this notary office did not adopt internal procedures referring to the minimum safety requirements for personal data processing adopted according to Order no. 52/2002 on approving the minimum safety requirements for personal data processing.

According to the findings, at the date of the investigation, there was no method of authentication required in order to access the computers where the notary documents were drafted. At the same time, the documents could have been copied on any external support and printed by any person having access to the computer. The non-existence of authentication methods indicates that any person could have access to any personal data existent on any computer from that notary office and thus, it was impossible to identify the persons who had access to the IT devices from the logs. Moreover, there was the possibility to copy any document on an external device and, as a consequence, to infect with viruses from the external storage devices used.

The controller was sanctioned for the contravention provided by Article 33 of Law no. 677/2001, because the controller did not adopt, until the day of the investigation, sufficient security and confidentiality measures in order to protect the personal data of the clients, employees, and its collaborators (including sensitive data) against unauthorised disclosure and access, as well as against any form of illegal processing as Article 19 and 20 of Law no. 677/2001 provide, which determined the disclosure of such personal data on the Internet.

SLOVAKIA



A. Summary of activities and news

The first half of 2013 is characterised by continuing efforts to change data protection legislation and the second half by application of adopted laws into practice. 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 an entirely new draft of the Act on personal data protection. The Objective of the changing of the act was to completely transpose the Directive of The European Parliament and the European Council 95/46/EC and implement conclusions and recommendations of Schengen evaluation in the Slovak Republic in the personal data protection area and law analysis from an application practice point of view. This legislative process finished in April 2013 when the Slovak National Parliament adopted a new Act on Personal Data Protection under the number 122/2013 Coll.

The Act entered into force on 1 July 2013 and brought several important changes, for example better specification of controller’s and processor’s status as well as relations between them, and newly regulates requirements for the processing of biometric data, clearly defines the scope and documentation of security measures, specifies the institute of the entitled person (a person entering into contact with personal data at the controller), newly regulates requirements for appointing a Data Protection Officer (the new PDP Act sets mandatory passing of an examination in order to exercise this function at the Office), strengthens the mechanisms for protection of a data subject’s rights, changes the conditions for the cross-border flow of personal data, specifies conditions for the notification and special registration of filing systems, introduces an administrative fee for special registration, further specifies the position of the Office, and extends its scope of competencies in the area of personal data protection, etc.

The Office further continued the weekly services of monitoring and assessment of materials included in the legislative process within the inter-ministerial review proceeding. The aim of this process is to 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 so that the basic requirements of social life were legally protected while interference in regard to the right to privacy and the privacy of individuals was minimised. For this purpose, every legislation draft that governs by its content the processing of personal data must comply with the basic requirements of the Act on personal data protection.

The adoption and implementation of a new act on personal data protection increased the interest of all stakeholders in personal data protection. Requests for information on this issue increased enormously in second half of 2013. The Office had to answer, in writing, 2 263 requests in total, of which 1 671 referred to the new act. The response by telephone can be counted in dozens per day. The obligation to pass an exam at the Office for persons wishing to perform a function of DPO has also contributed to increased interest, discussion, and better data protection. The Office organised training for controllers, processors, DPOs, or entitled persons within the whole country to satisfy the requirements of the knowledge of the law.

Nationwide inspections activities of the Office

During the year 2013, the Office carried out several nationwide inspection operations based on the annual plan of control activities as well as on the instigation of data subjects, state authorities, or other persons. The annual control activities plan was focused on the inspections of personal data processing in filing systems for ex. in the area of social services, local self-government, financial services, or CCTV. Seeing that the national law changed in the middle of 2013, the inspections have been divided into two parts. The first part was performed pursuant to Act No. 428/2002 Coll. and the second was pursuant to

Act No. 122/2013 Coll. on Personal Data Protection due to the fact that the provisions on both inspections and control procedures differ.

The national unit of SIRENE

Based on the 3rd provision of the Schengen Action Plan of the Slovak Republic, the Office investigated the lawfulness of personal data processing in the Schengen Information System of the second generation, to which the Slovak Republic joined on 9 April 2014. The inspection was aimed at conformity of data processing within an appropriate legal framework and the security of processed personal data. The Office also controlled the scope of processed personal data on persons wanted for arrest for the purpose of surrender or extradition, on residents of third countries in relation to the refusal of entry or stay, and on persons and things for the purpose of discreet surveillance or specific checks. The office revealed that the security of personal data processing is at a high level and fully complies with the relevant legal framework.

The area of social services

The Office aimed its supervisory activity in 2013 toward areas in which the controllers process not only general personal data but also data regarding special categories. The area of social services is one which demands the particular attention of the Office due to all of the related organisations (controllers) processing a significant amount of data related to special categories. The inspections in this area followed the inspections from the previous year and showed that the controllers neglected to fulfil some administrative obligations pursuant to Act No. 428/2002 Coll. such as instructing the responsible persons working with personal data of their obligations, keeping a register when using filing systems, or not appointing a data protection officer, etc. The Office issued corrective measures and started a procedure to impose a fine after five inspections.

Local self-governments

The local self-governments belong to a type of controllers that process special categories of data according to many national acts. They keep a register of citizens, collect local duties and fees, provide social assistance and benefits, provide other municipal services, etc. All of those activities require the processing of special categories of data and the local self-government is able to recognise the full economic, social, racial, or health situations in regard to the related data subjects. The Office has performed 10 inspections and 9 of them were finished with a protocol for corrective measures. Apart from omitting administrative obligations, the controllers have published personal identification numbers of data subjects onto their web sites, disclosed the economic situations of data subjects during sessions of local parliament, failed to indicate that the public area is monitored by CCTV cameras and, in one case, the controller did not comply with any legal obligations.

Financial services

The Office performed 3 inspections pursuant to Act No. 428/2002 Coll. and 8 inspections pursuant to Act No. 122/2013 Coll. in the area of financial services. The controllers processed personal data mainly according to special act No. 186/2009 Coll. on financial brokering and counselling. This Act allows for the processing of data in special categories and, for this reason, the Office put an increased amount of surveillance on this sector. The main issues related to data processing by processor, the determination of the scope and terms of processing, collection and processing in conflict with the law, and the usage of data for different purposes without notifying the data subject.

Cross-border Personal Data Flow

Act No. 122/2013 Coll. also changed the conditions for cross-border data flow. The concept was reworked to more closely adhere to the modern version which allows for a higher level of flexibility and decreases the administrative burden. Of course, the law distinguishes between transfers to the member

states of the European Union and to the countries which are contractual parties of The Agreement on the European Economic Area, and makes transfers to the third countries according to decision of the European Commission which ensures an adequate level of protection. It also makes transfers to the third countries that do not ensure an adequate level of data protection. Cases of cross-border data flow within the EU and third countries also ensure an adequate level of protection. The Act only requires the existence of an applicable legal base for exercising this processing operation, and the obligation for fulfilment falls on the controller to inform the data subject and ensure their data security during the transfer. There are no other limitations for this type of cross-border transfer. Transfers to a third country which do not ensure an adequate level of protection may be realized only if the controller provides sufficient guarantees for protection of privacy and the fundamental rights and freedoms of individuals. Binding corporate rules and standard contractual clauses are considered to be sufficient guarantees for those transfers.

The level of administrative burden was reduced by a new mechanism of prior authorization for cross border transfer to a third country which doesn't ensure an adequate level of protection. In the past, the controller had to ask for prior authorization for all transfers to a third country without an adequate decision pursuant to Act No. 428/2002 Coll. Now, it is necessary to request an authorisation of the Office only in cases when the controller intervenes in the content of standard contractual clauses or in cases where there is an apparent discrepancy.

Organisation	Office for the Personal Data Protection of the Slovak Republic
Chair and/or College	Eleonóra Kročianová, President
Budget	€876 324
Staff	33 employees
General Activity	
Decisions, opinions, recommendations	The Office issued the following six recommendations in 2013: 1/2013 The concept of personal data 2/2013 Basic concepts – people in personal data processing 3/2013 CCTVs in private cars 4/2013 Cross-border transfer of personal data 5/2013 The concept of filing systems 6/2013 Processing of biometric data
Notifications	387
Prior checks	28
Requests from data subjects	160 complaints and requests from data subjects 34 complaints and requests from other subjects
Complaints from data subjects	
Advice requested by parliament or government	108
Other relevant general activity information	The Office provided 7 speeches over radio, 9 on national television, and 58 contributions to printed media.

Inspection Activities	
Inspections, investigations	163 inspections
Sanction Activities	
Sanctions	151 decision on corrective measures
Penalties	11 penalties totalling €25 160 9 penalties for administrative offenses totalling € 20 360 2 fines totalling €3 500
DPOs	
Figures on DPOs	The Office performed 253 exams of DPOs during the establishment of the Office and 47 in other parts of the country for 3 073 applicants in total and the Office issued 1705 certificates of successful completion of tests.

B. Information on case-law

The legal system of the Slovak Republic, as with the legal systems of several other Member State, is not based on case-law.

C. Other important information

International Cooperation

Tasks at the international level resulted mainly from the membership of the European Union and in working groups established under the auspices and from legal acts of the European Communities as well as from requests for partnership and cooperation from the DPA. The Office participated in all meetings organised by the Council of Europe, Council of the European Union, or European Commission in 2013. In addition to regular meetings of working groups, the Office attended the Central and Eastern Europe Data Protection Authorities Conference, Spring Conference in Lisbon, Case Handling Workshop in Sarajevo, and organised a bilateral meeting with the DPA of the Czech Republic. Both DPAs tried to find cases with common issues that could be investigated in a coordinated manner and signed a Memorandum of Understanding at the end of the meeting.

SLOVENIA



A. Summary of activities and news

The year 2013 marked the tenth anniversary of operations for the Information Commissioner, whose role has grown through these years from one of a small scale appeals body headed by the Commissioner for Access to Public Information, to one as an important guarantor of transparency and the protector of personal data. In addition, 2013 brought with it a number of important milestones, which helped us comprehend just how very much we can lose when we surrender our privacy. Notable incidents, related to invasions of privacy, revealed how major invasions into our privacy occur, in effect, every day, and how powerless we are as individuals if the state loses its control in this area.

In 2013, the Information Commissioner received 106 requests for opinions on legislative proposals and other regulations that provide for personal data collection and processing (26 more than in 2012). We detected a disturbingly large number of amendments to acts and proposals for new acts, which would enable serious intrusions into the privacy of individuals in terms of the processing of personal data, which are being adopted using fast-track procedures without appropriate analyses and assessments of their consequences for ensuring the constitutionally guaranteed protection of privacy and personal data of individuals. Among the acts that have been in the process of amendments are the Criminal Procedure Act, the Removal and Transplantation of Human Body Parts for the Purposes of Medical Treatment Act, the Electronic Commerce Market Act, the Prevention of Undeclared Work and Employment Act, the Health Care and Health Insurance Act, the Patient Rights Act, the Minor Offences Act, and the General Act on Data Retention on the basis of paragraph 4 of Article 165 of the Electronic Communications Act.

This past year, in both fields of its operation, the Information Commissioner has once again received a large (record) number of applications from individuals, covering requests for opinions, complaints and appeals. On the one hand, this is gratifying as it clearly indicates that individuals are becoming more and more aware of the purpose and importance of both of the human rights dealt with within the competences of the Commissioner. At the same time, we cannot ignore the fact that again in this past year, the marked increase in the number of complaints and inspections carried out can be attributed to the continuing trend of troubling practices by responsible authorities in the area of access to public information, while on the other hand we have the increasingly unmanageable appetites of a wide variety of data controllers, both private and public, eager to gather and process personal data.

The response from individuals confirms that the Commissioner's work has been effective. Public Opinion Research Center Politbarometer carried out a public opinion poll in January 2013, which included an assessment of the national supervisory authorities' performance. The public opinion poll indicated that the performance of several independent supervisory authorities (including the Information Commissioner) was assessed as extremely and highly positive by respondents (as opposed to the assessment of the functioning of the central state bodies (the National Assembly, the Government, and the President of the Government). It should not be overlooked that the Information Commissioner also ranked highest among the central government and social institutions most trusted by Slovenians in public opinion polls in 2010, 2011, and 2012, which shows an established confidence from the people in regard to the work of the Information Commissioner.

With regard to the area of personal data protection for 2013, the Information Commissioner dealt with 712 inspection cases and 106 offence procedures. In 2013, the Commissioner gained competence for monitoring and inspection on legislation regulating cookies. In mid-June 2013, the provisions of the Electronic Communications Act on cookies, which relate to the retention of information or the gaining of access to information stored in a subscriber's or user's terminal equipment, entered into force. After the cookies' provisions came into effect, the Information Commissioner had, by the end of 2013, received 35 complaints relating to 141 responsible organisations (website operators). Complaints were mostly related to inadequate or a complete lack of notice and inappropriate mechanisms for obtaining consent. Websites did not always provide adequate control mechanisms that would actually allow or prohibit the

installation of cookies. In particular, there were several cases where a website installed cookies, for which, following the entry into force of the new Electronic Communications Act provisions, the explicit consent of the user is required. Especially problematic were not only advertising and analytical cookies, but also cookies of certain plug-ins that are, as a general rule, installed by third parties and that allow recording of the user's everyday on-line activities across several different websites ("tracking cookies"). The vast majority of responsible organisations, against which the Information Commissioner initiated inspection procedures, corrected the identified irregularities or violations upon being informed of them, thus the Information Commissioner was not required to issue regulatory decisions. In cooperation with responsible entities, the Information Commissioner developed Guidelines for the use of cookies and answers to frequently asked questions, which were posted on the Information Commissioner's web pages. We received many questions from website operators about web analytics, namely how to implement them so that they would be allowed on the basis of implicit consent during the first visit. The Information Commissioner succeeded in the withdrawal of some of the more invasive plug-ins, primarily in respect to public sector websites and major Slovenian media websites.

In addition to complaints filed in the relevant period in connection with cookies, in 2013, as in previous years, the largest number of complaints received by the Information Commissioner related to video surveillance and the use of personal data for direct marketing purposes. Apart from the above mentioned complaints, particular attention must be drawn to complaints that were filed regarding the transfer and, consequently, reading of e-mails sent to the company e-mail addresses of employees; complaints that were filed regarding the publication of personal data on the websites of data controllers; complaints that were filed regarding the sending of payable SMS messages; and complaints that were filed regarding the processing of inaccurate and outdated data.

New challenges for personal data protection continue to be present in the field of modern information and communication technologies. This mainly concerns the wider use of remotely piloted automated systems, which enable concealed, difficult to detect and extensive collection of personal data and significant invasions of privacy. Since these remotely piloted automated systems can be equipped with a wide variety of sensors that enable capture of videos, images, sound and data on temperature, movement, location, etc., their use will represent a major challenge for the regulators as well as the guardians of privacy.

An important part of the activities of the Information Commissioner also relates to the introduction of new powers granted to law enforcement authorities, particularly with regard to very frequent changes in the regulation of criminal proceedings.

The Information Commissioner notes that there are still many difficulties in interpreting communication privacy, and points out that a written request from a state authority is not sufficient to obtain information on the identification of communicating individuals, as this area falls within the provisions of Article 37 of the Constitution of the Republic of Slovenia. The Article provides that the confidentiality of correspondence and other means of communication shall be guaranteed and that only on the basis of a court order may the protection of the confidentiality of correspondence and other means of communication and the inviolability of personal privacy be suspended where such is necessary for the initiation or during the course of criminal proceedings or for reasons of national security. At the end of 2013, the Information Commissioner published a report which revealed disturbing practices by the police, who in 2012, despite the clear provisions of the Electronic Commerce Market Act and the Criminal Procedure Act, on the basis of 35 written requests, requested data from information society service providers concerning users of websites with content that is supplied or transmitted by users of the service. In 31 cases, this was done without the necessary court order, while 30% of written requests did not qualify in regard to the criminal offence in question.

Organisation	Information Commissioner of the Republic of Slovenia
Chair and/or College	Mrs. Nataša Pirc Musar
Budget	EUR 1 291 010
Staff	32 employees: the cabinet (2 to 6 of the employees were also supervisors, and 2 were legal advisers) administrative (3), access to public information and data protection legal advisors (10), researchers (2), data protection supervisors (10) and 1 system administrator.
General Activity	Data protection and access to public information
Decisions, opinions, recommendations,	71 comprehensive and 2 389 short opinions and recommendations based on requests from data subjects or data controllers.
Notifications	134 notifications on personal data filing systems.
Prior checks	23 prior checks: 11 on biometrics, 16 on transfer of data to third countries, 5 on connection of filing systems.
Requests from data subjects	2 460 requests for opinions/clarifications from data subjects.
Complaints from data subjects	852 complaints from data subjects altogether. Areas: 68 regarding unlawful transfer or disclosure of data, 43 regarding unlawful collection of data, 28 regarding cookies, 26 regarding inadequate data security, 15 regarding unlawful video surveillance and inappropriate use of video footage, and 7 regarding direct marketing. 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 106 acts and other legal texts, among others the Criminal Procedure Act, Removal and Transplantation of Human Body Parts for the Purposes of Medical Treatment Act, Electronic Commerce Market Act, Prevention of Undeclared Work and Employment Act, Health Care and Health Insurance Act, Patient Rights Act, Minor Offences Act, and General Act of Data Retention on the basis of paragraph 4 of Article 165 of the Electronic Communications Act.
Other relevant general activity information	The Commissioner in 2013: <ul style="list-style-type: none"> - continued its preventive work (lectures, conferences) on safe internet use for children, pupils, their parents and teachers together with the Centre for Safer Internet; - continued with education of responsible entities and participated in various educational conferences, workshops and round tables; - published Guidelines on intelligent video analytics and Guidelines on the use of cookies on websites;

	<ul style="list-style-type: none"> - was consulted regarding a number of acts; - continued strong international involvement and participation.
Inspection activities	
Inspections, investigations	712 inspections: 253 in public sector, 459 in private sector.
Sanction activities	
Sanctions	106 offence procedures initiated (18 in public sector, 62 in private sector, 26 private persons), of these 26 warnings and 72 decisions on a violation (36 admonitions and 36 fines).
Penalties	The DPA imposed 224 592 329 eur of penalties, administrative taxes excluded.
DPOs	
Figures on DPOs	N/A

B. Information on case law

Recording of telephone conversations by a public institution

The Information Commissioner initiated an inspection procedure against a public institution after establishing that, as the responsible authority, it had installed an automated information system for calls to its contact centre phone number, which prior to allowing callers to talk to a contact centre officer, informed them that their conversation would be recorded to ensure quality of service. The inspection procedure established that the responsible authority had introduced the recording of telephone calls with a view toward maintaining and improving quality of service. The audio recordings of the telephone conversations were used to prepare proposals for a training program for call centre operators (rhetoric training, dealing with clients in difficult situations, etc.). The Commissioner concluded that despite giving prior notice of recording, the responsible authority had no legal basis for these particular recordings. Therefore, the Information Commissioner ordered the authority to stop recording telephone conversations at its call centre phone number, to destroy stored recordings and also to stop using the automated information system notification “To ensure quality of service your call is being recorded”.

Inadequate security of sensitive personal data by a health care institution

The Information Commissioner carried out an inspection visit at a health care institution, the purpose of which was to verify the adequacy of procedures and measures to protect personal data. During the inspection, the Information Commissioner found that internal documents regulating security of personal data did not determine the procedure for keeping or using audit trails of access to personal data. The Information Commissioner found that in its database of personal data the responsible authority processed a large amount of personal data, a large proportion of which were, with regard to the authority’s field of activity, sensitive personal data, whose misuse could have serious, time-consuming and, in some cases, irreversible consequences for the individual. Given the sensitivity of the data processed by the responsible authority, any risk analysis should have shown that these are data with a high or perhaps the highest level of risk, and therefore measures and procedures to protect such personal data at the highest level should have been in place to mitigate the risks to which they are exposed. The Information Commissioner therefore ordered the authority to formalise a protocol for the

implementation of internal audits in an internal document, defining its scope, frequency, persons responsible, goals, manner of implementation, reporting and required action in the case of perceived unlawful processing of personal data.

During the inspection, it was also found that the responsible authority, for the purpose of access to the information system which consequently allowed traceability of the personal data processing, was using a system of user names and passwords that did not expire, and to which all doctors and nurses had the same access rights. Any doctor could view data on all patients who were or are still being treated at the responsible authority. Additionally, there were no requirements regarding the complexity of the chosen password, thus deviating from accepted good practices in the field of IT and information security. Considering the nature of the personal data processed by the responsible authority in the information system, and taking into account the risks posed, such practices are unacceptable. Consequently, the Information Commissioner ordered the authority to include password policy in an internal act and to start implementing it.

Police powers in the case of access to web users' data

The Information Commissioner received a complaint related to the use of police powers in connection with the acquisition of data on users of websites which have content that is submitted by service recipients or users (these are websites such as on-line forums, media websites, etc.). The complaint raised suspicions that in an unknown number of cases personal data of users of on-line forums had been obtained without the proper legal basis. Based on the analysis of the data provided by the police, the Information Commissioner noted that the police were not using the correct legislation for the acquisition of personal data from on-line forum operators who are information society service providers (and not from operators of electronic communications networks). They were using provisions of the Criminal Procedure Act, Police Act or even Personal Data Protection Act instead of the Electronic Commerce Market Act, which regulates obtaining information from information society service providers. In some cases there was no legal basis indicated at all. It was also evident that there was a lack of knowledge of the differences between the operators (providers of publicly available electronic communications networks and services) whose operation is primarily governed by the Electronic Communications Act, and operators of websites (information society service providers) whose operation is primarily governed by the Electronic Commerce Market Act. The Information Commissioner informed the Ministry of the Interior and the Office of the State Prosecutor General of the Republic of Slovenia of the findings of the inspection and suggested the preparation of a report in response thereto which would include a list of measures to address the identified deficiencies. By the end of 2013, the Information Commissioner received an interim report from the Ministry of the Interior. The case continued to be addressed in 2014.

Loss of voters' signatures to a call for a legislative referendum

Following media reports on the missing lists with signatories, calling for a legislative referendum on the Act Defining the Measures of the Republic of Slovenia to Strengthen Bank Stability, the Information Commissioner initiated an ex officio inspection procedure at the National Assembly and the Ministry of the Interior regarding the implementation of the provisions of PDPA. In the course of the inspection, it was found that the number of signatures or the number of sheets of paper the list of initiators (i.e. signatories) was comprised of was not properly verified or documented by the National Assembly upon the acceptance or upon photocopying and releasing the list to the Ministry of the Interior or the authenticity of signatures to be verified. The Ministry also did not appropriately document and verify the actual size of the list with personal data upon receipt of photocopies, its distribution among the employees for verification, or upon its returning following verification of the list. It was only after the intervention of the initiator in response to the apparent insufficient number of signatures, that an internal verification was carried out at the National Assembly and sheets were counted, establishing that the original list of signatures received was comprised of 307 sheets of paper; while the Ministry of the

Interior returned photocopies of 271 sheets that had been verified. Therefore, it was established that 36 photocopied sheets with personal data of 361 signatories were missing. The Information Commissioner established that both responsible authorities had acted contrary to the requirements of PDPA on procedures and measures to protect personal data, as they failed to verify and record the size and content of the list of signatories to the voters' initiative calling for a legislative referendum. Additionally, the authorities failed to provide so-called external traceability as they did not ensure that it would be possible to subsequently establish what personal data of signatories of the initiative had or had not been delivered to the other responsible authority. Due to the irregularities identified, the Information Commissioner imposed a sanction against the responsible persons at the National Assembly and at the Ministry of the Interior.

Premature destruction of medical records

On the basis of a complaint, the Information Commissioner initiated an inspection procedure against a responsible entity (a health spa) because of the claimed unlawful destruction of an individual's medical records just three years after their treatment was completed. During the inspection it was established that the internal acts of the responsible entity set different retention periods (5 – 15 years) for personal data of health service users. Despite these retention periods, the responsible entity, due to limited space and limited technical possibilities for storage of very large quantities of medical records in paper format, only kept medical records for three years after the completion of the health spa treatment. The medical records intended for destruction were weighed, but no list of patients' names, whose records were destroyed, was produced due to the very large number of cases (approx. 2,500–3,000). The Information Commissioner found that health spas are, in accordance with the relevant legislation, considered health care providers, so they must comply with the provisions of a special law, i.e. ZZPPZ, regarding the storage of personal data. According to ZZPPZ, the patient record and clinical history are to be stored for 10 years after the death of the patient, while other basic medical documentation is to be stored for 15 years. The Information Commissioner also received an opinion of the Ministry of Health that the medical documentation generated in health spas should be considered part of the patient record and clinical history, which should be retained for 10 years after the death of the patient. The Information Commissioner ordered the responsible entity to ensure that the personal data of their health service users would be stored and destroyed in accordance with the provisions of ZZPPZ, i.e., 10 years after the death of the user. The entity was also ordered to ensure such traceability in a way that, for every destruction, it will be clear when the destruction was carried out and the data of which persons were destroyed (first and last name of the patient, patient record number). The problems of lack of space and traceability can easily be solved by storing the data in an electronic form, as ZZPPZ does not prescribe the form in which health care providers must store records with personal data.

Publication of customer personal data on a repairer's "Welcome screen"

The Information Commissioner found that a vehicle repair shop (the responsible entity) was using an electronic booking system and that the following customer personal data appeared on the "Welcome screen": name and surname of the customer, time of admission of the customer, make of customer's vehicle, vehicle registration number, and name and surname of customer's service advisor. According to the organisation, the above mentioned screens were intended for customers to see when their vehicle will be accepted for service and which service advisor they should contact. The customers were satisfied with the introduction of the screen, so in the opinion of the organisation, the use of the screen represented a necessary organisational measure that saved customers time and money, and enabled repair technicians to better prepare for work and thus improved service. The Information Commissioner pointed out that the use of a certain technology which incorporates the processing of personal data, must also be considered in terms of the purpose of its use. If the purpose of the data controller is to process the personal data of individuals (name and surname of the customer and the vehicle registration number), then by its very nature this represents the processing of personal data for which the processor must have a proper legal basis. Publication of personal data on the "Welcome screen"

represents the communication, dissemination, and making personal data available to anyone who is in the premises of the repairer at the time of publication of the data. Such processing is certainly not necessary or appropriate for fulfilling contractual or any other obligations of the responsible entity nor is it necessary for the fulfilment of the lawful interests of the private sector, which means that the responsible entity had no legal basis for it. Furthermore, the organisation had no basis in law nor the personal consent of the individual for such processing. The Information Commissioner ordered the responsible entity to stop publishing the personal data of its customers – contracting parties (name and surname of the customer with the vehicle’s registration number) on its so-called “Welcome screen” in all its service units or instead to obtain express personal consent from each individual customer for such processing of their data.

C. Other important information

The Information Commissioner’s 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.

Due to budgetary cuts, in 2013 the Information Commissioner participated in only the most urgent European Union plenary meetings and occasionally attended meetings of four of the many subgroups of the Article 29 Working Party. In total, the Information Commissioner participated in eight EU working bodies dealing with control over the implementation of personal data protection in the context of individual areas of the EU, namely:

- the Article 29 Working Party for personal data protection, as well as in four of its subgroups (Technology Subgroup, Future of Privacy Subgroup, Binding Corporate Rules (BCR) Subgroup, and 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 SIS II;
- 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 national authorities for the protection of personal data for the supervision of VIS;
- at co-ordination meetings of the European Data Protection Supervisor (EDPS) together with state national authorities for the protection of personal data (EURODAC).

In March 2013, the Head of the Information Commissioner was elected Chairman of the Europol Joint Supervisory Body. The Information Commissioner also actively participated in the International Working Group on Data Protection in Telecommunications (IWGDPT), which brings together representatives of Information Commissioners and authorities for personal data protection and privacy from around the world. Once again, in 2013, a representative of the Information Commissioner participated in the Council of Europe’s Consultative Committee (T-PD) on the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108).

On 19 July 2013, the Head of the Information Commissioner Nataša Pirc Musar was appointed by the European Commission to a special ad hoc EU–USA group, whose task was to determine the actual level of activity of the US National Security Agency (NSA) in relation to the mass collection of information and personal data of European Union citizens. Nataša Pirc Musar participated in the special group as one of the five top European experts in the field of personal data protection. At the end of its mandate, the group prepared a report on its findings for the European Commission.

On the basis of Article 60 of Council Decision 2007/533/JHA on the establishment, operation, and use of the second generation Schengen Information System and Article 44 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), the Information Commissioner is responsible for independent monitoring of the lawfulness of the processing of SIS II personal data in their territory and its transmission from their territory. In 2013, the Information Commissioner received no complaints regarding the implementation of these rights in the first instance.

In 2013, the Republic of Slovenia conducted an evaluation of the implementation of the Schengen acquis in terms of personal data protection, in which the Information Commissioner actively participated.

In 2013, the Information Commissioner hosted representatives of similar institutions from Croatia, Bosnia, Herzegovina, and Macedonia. They were familiarised with the Commissioner's operation and good practice in the areas for which it is responsible.

In 2013, the Information Commissioner, as a leading partner, successfully completed Twinning Light Project SR/2009/IB/JH/01 – “Improvement of Personal Data Protection” in Serbia. In the context of international cooperation in the field of access to public information, in 2013 the Information Commissioner began a two-year participation in an international consortium in the LAPSI 2.0 project, which is intended to continue the work of the LAPSI 1.0 project and to establish a thematic network of experts in the field of the re-use of public information with the objective of removing obstacles to its implementation that occur in practice.

On 24 October 2013, the Information Commissioner organised an international conference on the theme of re-use of public information. The conference was organised within the framework of the European LAPSI project (Legal Aspects of Public Sector Information; <http://www.lapsi-project.eu/>), which is intended to establish a thematic network in the field of re-use of public information and is funded by the European Commission, and where the Information Commissioner, as one of its partners, cooperates. The purpose of the conference held in Ljubljana was to present new trends and challenges brought by the amendment to Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, with a particular focus on the issue of personal data. The event was also broadcast live over the Internet.

SPAIN



A. Summary of activities and news

After the constant increase of the last few years, in 2013 the activity of the Agency maintained the levels reached in 2012, notably with regard to complaints and inspection-related activities. Although numbers have suffered a slight reduction, figures remain high, with 10,600 complaints lodged by citizens and more than 10,700 final decisions issued by the Agency.

Throughout 2013, we have continued working on measures to promote knowledge and facilitate the exercise of the rights of citizens as well as to ease regulatory compliance. In that sense, the Agency opened a new thematic channel on its web site called “Protect your information online”, with a series of instructional videos in which it is shown, step by step, how to set privacy options browsers, social networks, and common system operations. Other materials will be loaded on to this channel in the future. The enlargement of the services offered via our e-services platform, launched in 2012, deserves particular reference, as well as the enhancement of all the information services provided through our website including the actualization of some of the most popular Guidelines addressed to controllers in different sectors.

With regard to inspection activities and the exercising of sanctioning powers, it is relevant to point out that, even though the figures on punitive resolutions remain quite stable, there has been a substantial increase in the percentage of decisions (84 % of the total) where the fine has been reduced by the application of the new criteria introduced by a law passed in 2011 to mitigate the severity of sanctions taking into account elements such as the behaviour of the controller, the existence of accountability measures, or the real consequences of the infringement. On the other hand, there has been a slight reduction in the number of decisions where the economic sanction has been replaced by a “preventive warning”, that now represents 24 % of all sanctioning decisions.

The Agency is also maintaining its effort on ensuring better protection for children. In that regard, in October 2013 it launched its new educational website aiming to offer relevant information and tools for both children and educators. The website reunites all previous educational materials published by the Agency and includes new tools specifically developed for this site.

Organisation	Spanish Data Protection Agency
Chair and/or College	José Luis Rodríguez Álvarez
Budget	13 524 070 €
Staff	158
General Activity	
Decisions, opinions, recommendations	
Notifications	602 531
Prior checks	n/a
Requests from data subjects	102 064
Complaints from data subjects	10 604

Advice requested by parliament or government	318
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	2 299
Sanction Activities	
Sanctions	874
Penalties	22 339 440
DPOs	
Figures on DPOs	n/a

B. Information on case-law

In 2013, the Audiencia Nacional (court of appellate against decisions made by the Agency) issued 274 resolutions, of which:

- 188 rejected the appeal against decisions of the Agency (68 %)
- 33 partially accepted the claim of the appellant (12 %)
- 53 totally accepted the claim (20 %)

The Supreme Court issued 12 sentences in cases of appeal against judgments of the Audiencia Nacional. In all cases, the sense of the sentence confirmed the position of the Agency.

The Audiencia Nacional Court also decided to address the EU Court of Justice for a preliminary ruling in a case involving the so-called “right to be forgotten”. The case is one of the nearly two hundred pending before the Court and refers to the complaint lodged by a citizen before the Agency against Google. The Agency issued a decision requesting Google to delete a number of search results. Googled appealed that decision.

There are two main issues at stake in the request for a preliminary ruling:

a. On one hand, the applicability of the Directive 95/46 focused on the services offered by Google Inc. to EU citizens. To that end, the Court tabled a battery of questions related to the applicability of the 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 in the territory of a Member state”. In that sense, the Court made direct mention to 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. 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 answer were yes, the second question would inquire about the real nature of the legal responsibilities of the entity offering the service... whether they were direct, full or simply a 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 of the affected information.

C. Other important information

In 2013, the Data Protection Agency of the Autonomous Community of Madrid discontinued its activity. Its competences have been returned to the State and assumed by the Spanish DPA.

Also, in relation to the scope of the activity of the Agency, the amendment of the law that regulates the Judiciary (Organic Law 4/2013) modifies the powers of its governing body (General Council of the Judiciary), including that one of “collaborating with the data protection Supervisory Authority in the field of the administration of justice. It will also assume the competences of that Authority only with regard to the activity of judges and magistrates in connection with the use of judicial files”.

On a different key, in 2013 the Agency concluded a sanctioning procedure against Google in relation to the company's new privacy policy. The procedure was opened in June 2013, in the framework of the coordinated enforcement reaction agreed on by the Working Party and led by the French CNIL. The final decision declared the existence of three serious violations of the Organic Law on the Protection of Personal Data (LOPD), imposed on Google a fine of 300,000 euros for each one of them, and requested that the company implement, without delay, the necessary measures to meet the applicable legal requirements. The three infringements refer to the unlawful collection and processing of personal information of authenticated, non-authenticated, and passive users; the storage and conservation of data for periods of time indeterminate or unjustified; and the absence of mechanisms for the exercise of the rights of access, rectification, cancellation, and opposition.



SWEDEN

A. Summary of activities and news

The attention paid to data protection issues from media, data controllers, and the public has increased in 2013. *Datainspektionen* has become even more visible in the news media and we have seen an increase in the number of subscribers to both our press releases and our magazine. We have held 62 seminars and lectures during the year which is an increase of 20 %. An increase is also shown in the number of proposals for new legislation which our DPA has been asked to give an opinion on, totalling 116 opinions. Also, on an international level, our work has become more extensive. The Commission proposal for a new data protection regulation has continued to be under discussion and our DPA has been following this work closely. The cooperation between the EU member states' data protection authorities has also continued to develop and the Swedish DPA takes part in several working groups in this field.

A significant event in 2013, was the entry into force of a new camera surveillance Act on July 1st. The new Act gives *Datainspektionen* a central responsibility for supervising camera surveillance and also the competence to appeal decisions from the county administrative boards to permit such surveillance. *Datainspektionen* has devoted a lot of resources to this and, in the second half of 2013, four employees were working full time on camera surveillance matters.

A major subject for debate in Sweden, and in other countries in 2013, was Edward Snowden's revelations about the monitoring of internet communications by the US NSA. Allegations that the Swedish Police was keeping records of persons with Romani origin also caused a big debate and lead to a field inspection by the specific supervisory board for the Police.

In our supervisory activity, one of our focus areas has been personal data processing by public authorities. This has included supervision of the exchange of information between authorities, the use of mobile devices and cloud services by public authorities, as well as developments related to e-government. Another focus area has been the Police, where we collected information about their personal data processing by sending questionnaires to all of the 21 regional police authorities. We also carried out field inspections at some of these regional authorities. Finally, we carried out an inspection of the Military intelligence services and their personal data processing in military intelligence activities for the first time.

Organisation	Data Inspection Board
Chair and/or College	Mrs Kristina Svahn Starrsjö, Director General
Budget	42 583 000 SEK = 4 288 750 €
Staff	Approx. 45 employees (= 41 full time equivalents)
General Activity	
Decisions, opinions, recommendations	26 decisions about permission to process data about criminal convictions (mostly concerning OFAC-lists) 64 opinions in consultation with data protection officials 214 decisions in inspection cases (see below) 2 checklists; personal data processing in recruitment databases and research activity
Notifications	3 378

Prior checks	44 (concerning personal data processing in research activity)
Requests from data subjects	230 formal requests, 6 100 e-mail questions, 7 100 phone calls
Complaints from data subjects	352
Advice requested by parliament or government	116 formal requests, around 70 informal consultations
Other relevant general activity information	53 press releases, 62 lectures and seminars
Inspection Activities	
Inspections, investigations	214
Sanction Activities	
Sanctions	---
Penalties	---
DPOs	
Figures on DPOs	7 047 controllers have appointed DPOs

B. Information on case-law

In March 2013, the County Administrative Court in Stockholm turned down an appeal from a security company who wanted to set up a database, a sort of “black list”, to prevent people from leaving petrol stations without paying for the fuel. *Datainspektionen* decided, in 2011, that such a database could not be permitted because of the vast registration of data, the risk of incorrect information, and the lack of means to have information rectified. The County Administrative Court confirmed this decision.

In the field of credit information, the County Administrative Court agreed with *Datainspektionen*’s previous decision to require strong authorization for subscribers that had access to credit information on the Internet. Two credit information companies disclosed information over the Internet and asked for usernames and passwords to provide access. *Datainspektionen*, and the County Administrative Court, said that this kind of disclosure required stronger authorization, such as e-id or non-reusable passwords.

Another court case regarding credit information concerned the obligation to provide a copy of the disclosed information to the person which the information refers to. When disclosing credit information over the Internet, the companies only provided a link to a website where this information could be read. In its decision, *Datainspektionen* said that this procedure is only adequate if it is optional and the individual accepts it and that, in other cases, a paper copy has to be sent by mail. The County Administrative Court took the same view.

C. Other important information

In the beginning of 2013, *Datainspektionen* gave an opinion on a report from a commission of enquiry who had examined the need for a review of the constitutional provisions on freedom of expression. In its opinion, the Swedish DPA suggested the introduction of a general provision that would criminalize severe

infringements of privacy on the Internet. We receive a great number of complaints from individuals who feel that their privacy has been infringed upon because of publications on the Internet. In many cases, we are unable to act because these publications are exempted from the data protection law for Freedom of Expression purposes. In our opinion, we expressed the view that a provision containing criminal sanctions for severe privacy infringements on web sites, etc. would help to prevent this behavior. During the year we have provided information for teachers to forward to their students about rights and obligations on the Internet. We have also held seminars for the police and for prosecutors to help in their investigations into severe privacy infringements on the Internet.

In November 2013, *Datainspektionen* celebrated its 40-year anniversary. The Swedish DPA was established in 1973 and was the first national data protection authority in the world.



UNITED KINGDOM

A. Summary of activities and news

The ICO has set five key aims for itself. Below are selected highlights about what we have done to meet those aims.

1. Organisations better understand their information rights obligations.

The ICO has published guidance on

- practice on subject access;
- direct marketing; and
- privacy impact assessments.

Amongst other issues we have been looking at Care.data, which is a system for general practitioners in England to release medical information to be used mainly for medical research and which has come under scrutiny. Our intervention led to improved patient information and revised timescales, but despite assurances it became clear that these mechanisms were not effective. We will continue to try to ensure that there are effective mechanisms in place to respect patient choices.

2. Enforcement powers are used proportionately to ensure improved information rights compliance.

We secured 12 criminal convictions and issued two cautions in the prosecution of the criminal offence of the unlawful obtaining or disclosing of personal data.

3. Customers receive a proportionate, fair, and efficient response to their information rights concerns.

This year we have received and closed a record number for cases. The ICO remains committed to ensuring improvements in information rights practices by using individual concerns to drive wider improvements. For example, we requested an action plan from the UK Banking Authority as an individual's request for their own information had taken over nine months to resolve. Additionally, we ensured that AXA PPP Healthcare revises its procedures for obtaining appropriate consent when processing medical information.

4. Individuals are empowered to use their information rights.

A cornerstone of data protection law is that of subject access. However, for some time this right has been misused by organisations, forcing individuals to apply for personal information and then to reveal it to the organisation. This enforced subject access is a perversion of rights intended for individuals and although provisions were included in the Data Protection Act 1998 to apply criminal sanctions these have never been commenced.

We have continued to press for change and the incoming Justice Minister, Rt Hon Simon Hughes MP, has now confirmed that other recent changes in the law have removed barriers and the way is clear to make enforced subject access an offence. We are working with the Ministry of Justice and others to ensure that this happens without further delay.

5. The ICO is alert and responsive to changes which impact information rights.

We provided advice on the proposed revision of the EU data protection regime to Ministry of Justice officials and to members of the European Parliament as well as worked through the Article 29 Working Party. An in-depth analysis of the latest proposals is on our website.

We also published research on the impact of the proposed revision on business which highlighted the uncertainty of many cost estimates being used in the debate:

- 40% of companies did not fully understand any of the ten main provisions being proposed and
- 87% were unable to estimate the cost of proposals to their business.

During the year, we consulted on the feasibility of the ICO accrediting a third party to run a privacy seal or certification scheme. This included work with the UK Accreditation Service. An announcement on the ICO’s proposed scheme will be made in 2014-2015.

6. An efficient ICO that is well-prepared for the future.

Significant new initiatives introduced this year helped us to work more efficiently and provide improved services to the public:

Our new registration system and service made the public register of data controllers more meaningful for those who visit it. It also became easier to use for those needing to register and we ended the year by launching a fully online registration service.

We made improvements to our telephone system to help us meet increased demand. We can now route callers to the right member of staff more efficiently and, if you call us outside of business hours, there is an improved automated service.

During the year we were increasingly proactive in disclosing information about our operational work.

Organisation	Information Commissioner’s Office
Chair and/or College	Mr Christopher Graham (Commissioner)
Budget	Approx. 21 million (Notification fee £16.5m and FOI grant in aid £4.25m)
Staff	370 FTE
General Activity	
Decisions, recommendations, opinions,	practice on subject access direct marketing privacy impact assessments
Notifications	Total data controllers notified 389 036
Prior checks	N/A
Requests from data subjects	Calls on helpline: 259 903

Complaints from data subjects	Number of complaints received for data protection: 13 760 Number of complaints received for freedom of information: 4 688 Number of complaints received for privacy and electronic communications act: 161 720
Advice requested by parliament or government	Responded to 44 consultations
Other relevant general activity information	None
Inspection activities	
Inspections, investigations	63 audits (and 117 advisory visits)
Sanction activities	
Sanctions	investigated 1 755 data protection cases issued 7 enforcement notices and 20 undertakings. 15 prosecutions (1 case resulted in confiscated funds totalling £73 000 to be repaid)
Penalties	issued £1.97m civil monetary penalties
DPOs	
Figures on DPOs	N/A

B. Information on case-law

N/A

C. Other Information

Other key highlights are as follows:

Student loans

The sale of the student loan book to the private sector could have resulted in a lot of unnecessary information about loans being disclosed to credit reference agencies. We worked to ensure that information on accounts which were up to date was not passed to credit reference agencies, and that there are effective safeguards to ensure the accuracy of any information transferred.

Online dating services

The use of online dating services has grown and there are concerns about how personal information is used and shared. We initiated work with the Online Dating Association to provide guidance to the sector.

Internet connected televisions

We are in contact with a television manufacturer to address concerns that information on viewing habits is being collected through internet-connected televisions even though privacy settings have been turned on.

Charities and community groups

We worked with charities and community groups supporting some of the most vulnerable people in society by giving presentations, advisory visits, and workshops.

Consulting Association

An important initiative for us this year related to a case we dealt with in 2009. Following the seizure of records held by The Consulting Association the ICO was in possession of information which had been used as a blacklist in the construction industry.

As well as addressing the data protection issues involved we were keen to contact those who may have been blacklisted. In many cases, given the passage of time, the information held seemed unlikely to allow us to accurately identify individuals. However, following work with both Equifax and the Department for Work and Pensions we were able to identify contact details for a number of those listed in the records.

Many other current and former construction industry employees and their representatives contacted us to find out if their details were held in the records we had seized. Between 2009 and 31 March 2014, we have provided 776 people with relevant information. Of these, some 461 were during the 2013/14 reporting year.

Working for greater consistency and coordination in the investigation and enforcement of global data protection issues

The ICO is also playing a leading role in improving the coordination of enforcement with other privacy regulators:

We co-chaired an International Enforcement Coordination Working Group which led to the adoption of a resolution driving this work forward at the International Conference of Data Protection and Privacy Commissioners. We are now leading the development of a set of rules for the exchange of information on enforcement activity.

We serve on the Executive Committee of the Global Privacy Enforcement Network.

We are represented in the OECD Working Party on Security and Privacy in the Digital Economy; contributing to its work on updating the OECD's privacy guidelines which have now been adopted by the OECD Council.

We signed a memorandum of understanding with the US Federal Trade Commission and one with the Dubai International Financial Centre Authority.

Changes to the way we deal with complaints

During the year we undertook a significant amount of preparatory work, including consultation, prior to making significant changes, in April 2014, to the way we deal with complaints and concerns raised by the public. The changes will allow us to take a more collaborative and proportionate approach to this important area of our regulatory work.

Chapter Three

European Union and Community Activities

3.1. European Parliament

3.1.1 Civil Liberties, Justice and Home Affairs Committee (LIBE) draft reports – 10 January 2013

The LIBE committee presented two draft reports on the reform of the EU's data protection rules proposed by the European Commission. Jan-Philipp Albrecht, rapporteur for the proposed Data Protection Regulation for the Civil Liberties, Justice and Home Affairs Committee (LIBE) of the European Parliament, and Dimitrios Droutsas, rapporteur for the proposed Data Protection Directive for the law enforcement sector, fully supported a coherent and robust data protection framework with strong and enforceable rights for individuals and stressed the need for a high level of protection for all data processing activities in the European Union to ensure more legal certainty, clarity, and consistency.

Key points include replacing Directive 95/46/EC with a directly applicable Regulation that covers the processing of personal data by both the private and public sector with single set of rules valid across the EU, support for a "one-stop shop" for companies that operate in several EU countries and for consumers who want to complain against a company established in a country other than their own and a powerful and independent EU data protection agency entrusted with taking legally binding decisions vis-à-vis national data protection authorities; support for strengthening users' rights; and applicability of EU rules where personal data of EU individuals is handled abroad by companies which are not established in the EU.

3.1.2 Industry, Research and Energy Committee (ITRE) report - 20 February 2013

The ITRE committee adopted its opinion on the Commission's proposals to reform the EU's data protection rules. This will now be submitted to the Civil Liberties, Justice and Home Affairs Committee (LIBE), which will consolidate all the amendments submitted so far and vote on its own report at the end of April.

The ITRE Committee backed the main innovations of the Commission's data protection reform. The ITRE opinion followed the publication on 10 January 2013 of the LIBE Committee's draft reports on the reform of the EU's data protection rules.

3.1.3 Legal Affairs Committee (JURI) opinion - 19 March 2013

The JURI committee adopted its opinions on the Commission's proposals to reform the EU's data protection rules. The opinions will be submitted to the Civil Liberties, Justice and Home Affairs Committee (LIBE).

The JURI Committee backed the architecture and the main fundamentals of the Commission's data protection reform:

The JURI opinions follow the publication of the draft reports on the reform of the EU's data protection rules by the LIBE Committee on 10 January 2013 and the votes in the ITRE, EMPL and IMCO Committees.

3.1.4 Civil Liberties, Justice and Home Affairs Committee (LIBE) reports – 22 October 2013

The LIBE committee adopted two reports on the reform of the EU's data protection rules proposed by the European Commission, giving its strong backing to the architecture and the fundamental principles of the Commission's data protection reform proposals, on both the General Data Protection Regulation and on the Data Protection Directive for law enforcement situations.

The LIBE vote gives a mandate to the Rapporteurs, MEPs Albrecht and Droutsas, to negotiate with the Council of the EU.

3.2. European Commission

On 27 November 2013, the European Commission presented a package setting out actions to be taken in order to restore trust in data flows between the EU and the US following concerns about revelations of large-scale US intelligence collection programmes, which have had a negative impact on the transatlantic relationship.

The package consisted of a strategy paper in the form of a Communication on transatlantic data flows setting out the challenges and risks following the revelations of US intelligence collection programmes, as well as the steps that need to be taken to address these concerns; an analysis of the functioning of Safe Harbour, which regulates data transfers for commercial purposes between the EU and US; a factual report on the findings of the EU-US Working Group on Data Protection set up in July 2013; a review of the existing agreements on Passenger Name Records (PNR); and a review of the Terrorist Finance Tracking Programme (TFTP) regulating data exchanges in these sectors for law enforcement purposes.

The Commission called for swift adoption of the EU's data protection reform; making Safe Harbour safer; strengthening data protection safeguards in the law enforcement area; using the existing Mutual Legal Assistance and Sectoral agreements to obtain data; addressing European concerns in the on-going US reform process; and promoting privacy standards internationally.

3.2.1 Rebuilding Trust in EU-US Data Flows

The Communication sets out six areas in which action is required:

A swift adoption of the EU's data protection reform: the strong legislative framework, as proposed by the European Commission in January 2012, with clear rules that are also enforceable in situations when data is transferred and processed abroad is a necessity now more than ever. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Making Safe Harbour safer: the Commission today made 13 recommendations to improve the functioning of the Safe Harbour scheme, after an analysis also published today found the functioning of the scheme to be deficient in several respects. Remedies should be identified by summer 2014. The Commission will then review the functioning of the scheme based on the implementation of these 13 recommendations.

Strengthening data protection safeguards in the law enforcement area: the current negotiations on an "umbrella agreement" for transfers and processing of data in the context of police and judicial cooperation should be concluded swiftly. An agreement must guarantee a high level of protection for citizens who should benefit from the same rights on both sides of the Atlantic. Notably, EU citizens that are not residents in the U.S. should benefit from judicial redress mechanisms.

Using the existing Mutual Legal Assistance and Sectoral agreements to obtain data: As a general principle, the U.S. administration should commit to making use of a legal framework like mutual legal assistance and sectoral EU-U.S. Agreements such as the Passenger Name Records Agreement and Terrorist Financing Tracking Programme whenever transfers of data are required for law enforcement purposes. Asking the companies directly should only be possible under clearly defined, exceptional, and judicially reviewable situations.

Addressing European concerns in the on-going U.S. reform process: U.S. President Obama has announced a review of U.S. national security authorities' activities. This process should also benefit EU citizens. The most important changes should be extending the safeguards available to US citizens to EU citizens that are not residents of the US, increased transparency, and better oversight.

Promoting privacy standards internationally: The US should accede to the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ("Convention 108"), as it acceded to the 2001 Convention on Cybercrime.

The Commission also makes clear that standards of data protection will not be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership.

3.2.2 Report on the Findings of the ad hoc EU-US Working Group on Data Protection

This report followed revelations as to the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data which concern the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US, which has the potential to significantly affect individuals in the EU.

Clarifications were requested from the US authorities on a number of aspects, including the scope of the programmes, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, as well as the different levels of protection and procedural safeguards that apply to US and EU persons. Subsequently, an ad hoc EU-US Working Group was established to ascertain the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens.

The US provided information regarding the legal basis upon which surveillance programmes were based and carried out, and clarified that the President's authority to collect foreign intelligence outside the US derived directly from his capacity as commander-in-chief, as well as from his competence in foreign policy as provided in the US constitution.

The report concluded that, under US law, a number of legal bases allowed large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. The number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes is unclear.

There are differences in the safeguards applicable to EU data subjects compared to US data subjects – collecting the data of US persons is generally not authorised. Where authorised, it is considered to be "foreign intelligence" only if it is necessary for that specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it relates to the purposes pursued. This results in lower thresholds being applied for the collection of the personal data of EU citizens.

The targeting and minimisation procedures are aimed at reducing the collection, retention, and dissemination of personal data of, or concerning, US persons, and do not impose specific requirements or restrictions with regard to the collection, processing, or retention of personal data of EU individuals. Oversight of the surveillance programmes aims primarily at protecting US persons. US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

Different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis). The use of other available legal bases, and the existence of other surveillance programmes, is not clear.

Since the relevant orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed about whether their personal data is being collected or

further processed. There are no opportunities for individuals to obtain access to, rectify, or erase data, or any administrative or judicial redress.

There is judicial oversight for activities that involve a capacity to compel information. There is no judicial approval of individual selectors to query the data collected or that which is tasked for collection. There is no judicial oversight of the collection of foreign intelligence outside the US, which is conducted under the sole competence of the Executive Branch.

3.2.3 Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU

In 2000, the Commission adopted Decision 520/2000/EC, recognising the Safe Harbour Privacy Principles and Frequently Asked Questions issued by the Department of Commerce of the United States as providing adequate protection for the purposes of transfers of personal data from the EU to the US.

The Safe Harbour decision therefore enables the transfer of personal information from the EU to companies in the US which have signed the Privacy Principles, in circumstances in which the transfer might otherwise not meet the EU requirements for an adequate level of protection of personal data. The functioning of the Safe Harbour arrangement relies on the commitments and the self-certification of member companies. Signing these arrangements is voluntary, but the rules are binding for those who sign. The fundamental principles of such an arrangement are transparency of the companies' privacy policies, the incorporation of the Safe Harbour principles in companies' privacy policies, and enforcement, including by public authorities.

Safe Harbour has to be reviewed as a result of the exponential increase in data flows, the rapid growth of the digital economy, and significant developments in data collection, processing and use; the importance of data flows to the transatlantic economy; the increase in the number of companies joining Safe Harbour (eight-fold since 2004), and information recently revealed about US surveillance programmes, raising questions on the level of the protection the Safe Harbour arrangement is deemed to guarantee.

The Communication is based on evidence gathered by the Commission, the work of the EU-US Privacy Contact Group in 2009, a study prepared by an independent contractor in 2008, and information received in the ad hoc EU-U.S Working Group established following the revelations of US surveillance programmes. It follows the Commission Assessment Reports in 2002 and 2004.

The Communication acknowledges that Safe Harbour has been a vehicle for EU-US flows of personal data, and US companies have hundreds of millions of EU clients, and the volume of transfers is on a scale which was unimaginable at the outset.

Areas requiring attention include transparency of privacy policies of Safe Harbour members, effective application of Privacy Principles by companies in the US, and effectiveness of enforcement. The large scale access by intelligence agencies to data transferred to the US via Safe Harbour certified companies also raises questions about the continuance of data protection rights of Europeans when their data is transferred to the US.

The Commission therefore recommended, as regards transparency, that:

- self-certified companies should publicly disclose their privacy policies;
- privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the current members of the scheme;
- self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, such as cloud computing services.

- the Department of Commerce website should clearly indicate all companies which are not current members of the scheme.

In relation to redress, the Commission recommends:

- the privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel;
- ADR should be readily available and affordable;
- the Department of Commerce monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedures they use and the follow-up they give to complaints.

Regarding enforcement, the Commission recommends that:

- following the certification or re-certification of companies under Safe Harbour, a certain percentage of these companies should be subject to *ex officio* investigations of effective compliance regarding their privacy policies (going beyond control of compliance with formal requirements);
- whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to a specific follow-up investigation after 1 year;
- in case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority;
- false claims of Safe Harbour adherence should continue to be investigated

As far as access by US authorities is concerned, the Commission recommends that:

- privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour; and
- the national security exception contemplated by the Safe Harbour Decision be used only to an extent that is strictly necessary or proportionate.

3.2.4 Terrorist Finance Tracking Programme (TFTP) evaluation report

In this report on the value of the data provided by the TFTP to counter terrorism investigations, the Commission concludes that the TFTP has generated significant intelligence that has helped detect terrorist plots and trace their authors. This information has been used to investigate the April 2013 Boston marathon bombings, threats during the London Olympics, and EU-based terrorists training in Syria.

TFTP data provides key insight into the financial support networks of terrorist organisations, helping to identify new methods of terrorist financing and persons involved in the US, the EU and elsewhere. EU Member States and Europol benefit from such information and receive valuable investigative leads. Over the last three years, in response to 158 total requests made by the Member States and the EU, 924 investigative leads were obtained from the TFTP.

Regarding recent allegations of access to financial messaging data in the EU contrary to TFTP agreement, written reassurances were received that the US Government had not breached the agreement and would continue to fully respect it. As at 2013, it was considered that there was no need for further consultations with the US on the implementation of the TFTP agreement.

Further to requests from the European Parliament and the Council, the Commission also assessed the options for establishing a European Terrorist Finance Tracking System (TFTS), weighing each option in terms of safeguarding fundamental rights, necessity, proportionality and cost effectiveness, as compared to the current situation.

It was concluded that there was no case for establishing such a system in the EU, *inter alia* because it would be necessary to create and manage a new database containing information about all EU citizens' financial transfers, and the database would raise serious challenges in terms of the data storage, access and protection, and technical and financial efforts.

3.2.5 EU US Passenger Name Record (PNR) Agreement joint review report

The EU-US PNR agreement on the transfer of air passengers' data for flights from the EU to the US entered into force on 1 July 2012. Following a review by EU and US experts, it was found that the US authorities had been implementing the agreement in accordance with the standards and conditions it contained.

The agreement provides an efficient tool to fight serious transnational crime and terrorism, while setting clear limits on what purposes PNR data may be used for, as well as a series of strong data protection guarantees.

The joint review report also finds that US authorities respect their obligations regarding access rights of passengers, and have a regular oversight mechanism in place to guard against unlawful discrimination. The masking and deletion of sensitive data are respected. The sharing of data with domestic US agencies and with third countries is in line with the Agreement.

3.3. European Court of Justice

3.3.1 [General Court: T-214/11 - ClientEarth and PAN Europe v EFSA \(on appeal\)](#)

Judgment of the General Court (Sixth Chamber) of 13 September 2013 - ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA).

In this matter the applicant sought access, pursuant to Regulation 1049/2001, to documents prepared by EU experts. The applicant knew the names of the experts, as well as the contents of the documents, but sought to find out which expert had made which comments. Disclosure of such information had been refused on the basis of Regulation 45/2001, which provides that access to documents could be refused where disclosure would undermine the protection of privacy and the integrity of the individual.

The applicants claimed that the institution in question had disclosed on its website the names, biographies, and declarations of interest in respect of each of the experts concerned and was therefore not personal data.

The Court held that the fact that individuals are listed on a publicly accessible website does not necessarily imply that their names can no longer be characterised as personal data.

The applicants further claimed that expert opinions have to be made public even if they might give rise to controversy or deter those who expressed them from making their contribution to an institution's decision-making process.

The Court held that it did not follow from that that the name of any expert who has commented on a European Union measure cannot be considered to be personal data.

3.3.2 [European Court of Justice: C-486/12 – X](#)

Judgment of the Court (Eighth Chamber) of 12 December 2013 - Proceedings brought by X.

In this decision, the Court held that Article 12(a) of Directive 95/46 does not preclude the levying of fees in respect of the communication of personal data by a public authority, as long as these fees are not excessive. Member States may fix that fee at a level which constitutes a fair balance between the interest of the data subject in protecting his privacy, in particular through his right to have the data communicated to him in an intelligible form, so that he is able, if necessary, to exercise his rights to rectification, erasure, and blocking of the data (in the event that the processing of the data does not comply with the directive) and his rights to object and to bring legal proceedings, and the burden which the obligation to communicate such data represents for the controller.

For the purposes of Article 12(a), where a national public authority levies a fee on an individual exercising the right of access to personal data relating to him, that fee should not exceed the cost of communicating such data. That upper limit does not prevent the Member States from setting lower fees in order to ensure that all individuals retain an effective right to access.

3.3.3 [European Court of Justice: C-473/12 – IPI](#)

Judgment of the Court (Third Chamber) of 7 November 2013 - Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others.

In this decision, the Court held that Article 13(1) of Directive 95/46 must be interpreted as meaning that Member States have no obligation, but have the option, to transpose into their national law one or more of the exceptions which it lays down to the obligation to inform data subjects of the processing of their

personal data, and its provisions in that regard are general and flexible, leaving to Member States to decide the details.

Member States are free to decide whether, and if so, for what purposes, they wish to enact in law exceptions for the purposes listed in Article 13(1)(a) to (g), including limitations on the obligation to inform the data subject. Such measures may only be laid down when they are necessary.

The situation of a private detective hired by a professional body to investigate breaches of ethics in a regulated profession is covered by Article 13(1)(d). Since the Directive does not specify how the investigation and detection of failures to comply with rules are carried out, it does not prevent a professional body from using investigators in performing its duties.

If this is laid down in national law, then neither the professional body nor the private detectives are obliged to inform the data subject as provided for in Articles 10 and 11. If it is not laid down, then data subjects must be informed.

Member States may also find that professional bodies and the private detectives acting for them are capable of performing their duties without relying on the exceptions in Article 13(1).

[3.3.4 European Court of Justice: C-342/12 – Worten](#)

Judgment of the Court (Third Chamber) of 30 May 2013 - Worten - Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT).

In this decision, the Court held that Article 6(1)(b) and (c) and Article 7(c) and (e) of Directive 95/46 do not preclude national legislation which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions so as to allow its immediate consultation, provided that this obligation is necessary for the purposes of the performance by that authority of its task of monitoring the application of the legislation relating to working conditions, in particular as regards working time.

[3.3.5 European Court of Justice: C-291/12 – Schwarz](#)

Judgment of the Court (Fourth Chamber) of 17 October 2013 - Michael Schwarz v Stadt Bochum.

In this decision, the Court held that Article 62(2)(a) EC, which was part of Title IV of the EC Treaty, authorised the Council to regulate how checks were to be carried out at the external borders of the European Union in order to ascertain the identity of persons crossing those borders. Such checks necessarily require documents to be presented that make it possible to establish that identity, Article 62(2)(a) EC therefore authorised the Council to adopt legal provisions relating to such documents and to passports in particular.

As regards the authority of the EU legislature in that area, the provision — which referred to checks on ‘persons’ without providing further details — was intended to cover not only third-country nationals, but also citizens of the Union and, hence, their passports.

Second, harmonised security standards for passports of EU citizens can be required in order to avoid passports having security features which lag behind those provided for by the uniform format for visas and residence permits for third-country nationals. In those circumstances, the EU legislature has the authority to provide for similar security features in respect to passports held by EU citizens, in so far as such authority helps to prevent those passports from becoming targets for falsification or fraudulent use.

3.4. EUROPEAN DATA PROTECTION SUPERVISOR

A: Summary of activities and news

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy;
- cooperating with similar authorities to ensure consistent data protection.

Ten years after its foundation, the EDPS is a mature organisation, able to address the many challenges of a data protection authority in a highly dynamic environment. Our main operational challenge in 2013 was that our activities continued to grow both in scale and scope while the budget restraints and resource measures due to the financial crisis were still in place.

Our [Strategy 2013-2014](#), together with our [Rules of Procedure](#) and Annual Management Plan, have been sources of valuable guidance, articulating the vision and the methodology required to improve our capacity to work effectively and efficiently in a climate of austerity.

A.1. Supervision and Enforcement activities

We saw an increase in the number of prior check notifications received in the context of our Supervision and Enforcement work. This increase is due primarily to the June 2013 deadline for *ex-post* prior check notifications for processing operations already in place. The increase in the number of Opinions we issued during the year is also a result of the high number of notifications received. We continued to follow up recommendations made in EDPS prior check Opinions already issued and were able to close a considerable number of cases.

The number of complaints we received decreased, partly due to better information and awareness of EDPS competencies, but also because of the effectiveness of our complaint submission form.

One of the features of the action plan as laid down in our Strategy 2013-2014 is to promote a 'data protection culture' within the EU institutions and bodies so that they are aware of their obligations and are accountable for complying with data protection requirements.

In light of this we continued to provide guidance and training to [controllers](#), data protection officers ([DPOs](#)), and data protection coordinators ([DPCs](#)) primarily in the form of [Guidelines](#) on Public Procurement, Grants and External Experts; basic training for new DPOs on the prior checking procedure; special training for the DPOs of five EU Joint Undertakings. Our awareness raising initiatives within EU institutions and bodies also included the organising of specific and general workshops.

Also key was our on-going dialogue with controllers, DPOs and DPCs to support the work of DPOs. These meetings help us gain a better understanding of the constraints of institutions in order to offer practical advice. Many meetings were held with controllers either in the course of prior check work or in the follow up to Opinions and decisions. The DPO network meetings, bilateral meetings and the helpline for DPOs were useful channels of communication for our work with the DPOs and DPCs.

A.2. Policy and Consultation activities

Throughout 2013, we continued to be closely involved in the on-going work on the reform of the [EU data protection framework](#). On 15 March 2013, we sent additional comments on the reform to the European

Parliament, the Commission and the Council. We also continued our involvement in the discussions that followed in both Parliament and Council.

In addition to this, the Commission published a large number of legislative proposals affecting the fundamental right to the protection of personal data.

We addressed the issue of the digital agenda and internet several times, for example, in our Opinion on the commission communication on the Digital agenda for Europe – Driving European growth digitally, our Opinion on the European Single Market for electronic communications and the Opinion on a green paper entitled “Preparing for a fully converged audio-visual world: Growth, Creation and Values”.

In the Area of Freedom, Security and Justice (AFSJ), we published Opinions on Europol, the EU cyber security strategy and smart borders as well as on EU-Canada passenger name records (PNR) and the European information exchange model.

Opinions of particular note relating to the internal market were our Opinions on anti-money laundering and terrorist financing, payments in the internal market, European company law and corporate governance and electronic invoicing in public procurement.

In the area of eHealth we would highlight our Opinions on medical devices, drug precursors and the eHealth action plan.

A.3. Cooperation activities

The EDPS cooperates with other data protection authorities in order to promote consistent data protection throughout Europe. This cooperative role also extends to cooperation with supervisory bodies established under the former EU “third pillar” and in the context of large-scale IT systems.

In 2013, we continued to actively contribute to the work of the Article 29 Working Party. In particular, we were heavily involved as rapporteur or co-rapporteur for the Opinions on purpose limitation and on legitimate interest (key provisions subgroup), the Opinion on the smart grid data protection impact assessment template (technology subgroup) and the Opinion on open data (eGovernment subgroup).

Direct cooperation with national authorities is also important for large-scale international databases such as EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) and the Customs Information System (CIS), which require a coordinated approach to supervision. In 2013, we provided the secretariat for the new SIS II Supervision Coordination Group (SCG) and we continued to chair the EURODAC, VIS and CIS SCGs. We organised two meetings in Brussels for each of the SCGs in 2013.

In addition, SIS II became operational. To reduce the financial, travel and administrative burdens, we established back to back meetings of the SCGs and aimed to ensure consistent, horizontal supervision policies of the large-scale IT systems where possible.

The SCG model will expand in 2014 with a new supervision coordination group for the Internal Market Information System (IMI). We consulted the national data protection authorities (DPAs) and the Commission in 2013 to take stock of the status and developments in the IMI Regulation in order to organise the first meeting for the group in 2014.

Within the framework of the Council of Europe, the EDPS attended three meetings of the Consultative Committee of the Council of Europe Convention 108. It was particularly important for us to attend these meetings to be able to follow and influence the on-going modernisation of the Convention.

The EDPS also took part in the experts group tasked with updating the privacy guidelines of the Organisation for Economic Co-operation and Development (OECD).

We also gave significant input on data protection issues in many other important fora such as the Asia-Pacific Economic Cooperation (APEC), the French-Speaking Association of Personal Data Protection Authorities (AFAPDP) and the International Working Group on Data Protection in Telecommunications (Berlin Group).

Organisation	European Data Protection Supervisor (EDPS)
Chair and/or College	Peter Hustinx, Supervisor Giovanni Buttarelli, Assistant Supervisor
Budget	7 661 409 Euro
Staff	62 (all categories of staff included)
General Activity	
Decisions, opinions, recommendations	20 legislative opinions issued on, among other things, initiatives relating to the Area of Freedom, Security and Justice, the Digital Agenda, eHealth, international cooperation and the internal market. 13 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. 33 sets of informal comments
Notifications	272 notifications of processing operations received from the Data Protection Officers of EU institutions and bodies for prior checking
Prior checks	91 prior-check opinions adopted notably on leave management, staff evaluation, recruitment, suspicion and offences, and procurement. 21 non prior-check opinions adopted
Requests from data subjects	176 requests for information and advice from the public or interested parties, the majority of which related to more information on privacy matters or assistance in dealing with problems such as the security of their personal information or the misuse of it.
Complaints from data subjects	78 complaints received, 30 admissible
Advice requested by parliament or government	The majority of the 20 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	37 consultations received on administrative measures relating to the processing of personal data in the EU administration. Advice was given on a wide range of legal aspects including transfers of staff data, change of purpose for data collected for a specific purpose and public access requests. A set of guidelines were issued on the processing of personal data

	<p>in the area of procurement.</p> <p>A number of training sessions and workshops were organised on specific subjects such as the role of a DPO, HR, IT and public procurement, the notification procedure and the prior check procedure. The workshops covered the use of electronic communication in the workplace, the use of mobile devices in the workplace, websites managed by the EU institutions and bodies and trans-border data flows.</p>
Inspection Activities	
Inspections, investigations	5 on-the-spot inspections and 2 visits carried out.
Sanction Activities	N/A
DPOs	
Figures on DPOs	62 DPOs in the EU institutions, bodies and agencies

B. Information on case-law

Court cases

In 2013, the EDPS intervened in a number of cases before the Court of Justice of the European Union and the Civil Service Tribunal.

The EDPS made oral submissions at a hearing before the Grand Chamber of the Court of Justice in a preliminary reference procedure. This hearing concerned the joined cases of Digital Rights Ireland (C-293/12) and Seitlinger and Others (C-293/12). Both cases relate to the validity of the Data Retention Directive 2006/24/EC.

It was the first time that the Court had invited the EDPS to appear at a hearing in a preliminary reference procedure. For the EDPS, this was an important step that may lead to a landmark decision on an issue that we have been following closely for a number of years.

The EDPS pleaded at the hearing of *Commission v. Hungary* (C-288/12). This case is the third infringement case on the independence of data protection authorities, the other two being *Commission v. Austria* (C-614/10) and *Commission v. Germany* (C-518/07) for which rulings were given in 2012 and 2010, respectively.

Other cases in which the EDPS intervened are still pending, such as *Pachtitis v Commission* and *EPSO* (T-374/07), *Pachtitis v Commission* (F-35/08), *ZZ v. EIB* (Case F-103/11) as well as *Dennekamp v. European Parliament* (T-115/13).

In October 2013, the EDPS asked for leave to intervene in two further cases: *Elmaghraby and El Gzaerly v. Council of the European Union* (Case T-319/13) and *CN v Parliament* (Case T-343/13).

C. Other important information

Review of the EU Data Protection Framework

Following our many activities on the [reform](#) in 2012, including our Opinion of 7 March 2012, we sent additional comments to the European Parliament, the Commission and the Council on 15 March 2013. Our comments related to specific areas that needed clarification and also reacted to the amendments proposed by the Members of the European Parliament to the European Commission's proposals.

In our comments, we advised against excluding specific sectors from the scope of application of the EU data protection framework and against limiting the territorial scope of the proposed general data protection Regulation. We also reiterated that pseudonymised data remains personal data (or personal information) and should be protected as such. Any definition of anonymous data or pseudonymous data should, therefore, be fully consistent with the definition of personal data and should not lead unduly to the removal of certain categories of personal data from the scope of the data protection framework. We supported the elimination of the potential further processing of data for incompatible purposes and stressed that the definition of explicit consent should be maintained. We also supported the definition and responsibilities of controllers and processors as proposed by the Commission, as well as the principle of accountability, which should apply to the whole package. Some of the elements of the so called *risk-based approach* were welcome but we pointed out that full protection as provided for in the Regulation should apply to all processing operations. As regards international transfers, we recommended that the rules be clarified and welcomed the amendments introducing a new article on transfers not authorised under EU law.

As regards the proposed data protection Directive on criminal law enforcement, we supported the closer alignment of the proposed Directive with the proposed Regulation to ensure consistency. We also welcomed the amendments introducing specific conditions and safeguards for access by law enforcement authorities to data initially processed for other purposes and highlighted that any transfer to non-law enforcement authorities or private parties should be strictly limited.

Following tough negotiations and many political compromises, on 21 October the LIBE Committee of the European Parliament adopted its report on the data. The report was endorsed by the European Parliament in first reading in its plenary vote of 12 March 2014. In Council, less progress has been made. Negotiations between Member States on important parts of the legislative framework such as the one-stop-shop mechanism and the scope of the Regulation and the Directive, among other politically sensitive and legally complicated issues, are continuing.

In the course of 2013, we continued to give advice to the European Parliament and the Council and contributed to the debate. We also contributed to the beginning of the process of revision of Regulation (EC) No 45/2001, which governs data processing carried out by the European Institutions, by sending a letter to the Commission outlining our initial views.

Chapter Four

Main Developments in EEA Countries

ICELAND



A. Summary of activities and news

The most imminent change in Icelandic data protection legislation that would have the most significant effect on the DPA's current work was a draft bill on scientific research in the health sector. The bill assumed that only the National Ethics Committee should issue permits for access to health data for the purposes of such research and that the DPA's role in that regard would cease. On the other hand, The National Ethics Committee should send the DPA a summary of issued permits for the DPA to decide which research projects it would like to inspect more closely. The National Health Committee would not be allowed to issue a permit until 10 days had passed since the aforementioned summary had been sent to the DPA. If the DPA notified the Ethics Committee about a further inspection of a specific research project, the Committee would be forbidden to issue a permit until the DPA had reached a conclusion on the matter. According to the bill, the DPA could give orders on security measures for the handling of personal data. Lastly, if the DPA thought that the processing of personal data for the purpose of scientific research contradicted Act no. 77/2000, on the Protection of Privacy as Regards the Processing of Personal Data, the Ethics Committee would be forbidden to issue a permit for a certain research project.

Another change in Icelandic data protection legislation was a modification of Act no. 163/2007 on Statistic Iceland, the centre for official statistics in Iceland. The bill on this modification entrusted Statistic Iceland with a very extensive collection of people's loans for statistical reports and also to form measures to be taken to benefit indebted homes. The DPA opposed such extensive processing and pointed out that the bill did not explain the necessity of such extensive dealings/interventions with people's privacy in order to reach the bill's goal – to form measures to benefit home-owners in debt. The Parliament took the DPA's observations into account and made changes regarding the protection of the data collected, preservation time, and erasure, among other things.

Finally, a change was made to Social Security Act no. 805/2013. What most concerned the DPA's field of work was a provision which expanded the Institution of Social Insurance's powers of supervision and collection of data from other governmental bodies such as tax authorities, the Directorate of Labour, the National Registry, certain pension funds, nursing homes, municipalities, the Icelandic Student Loan Fund, and other bodies and companies. The bill assumed that such data collection would be carried out without an individual's consent opposite to what had been done before. The DPA stated that the bill's provision on data collection, without consent, was too wide and open since it neither stated exhaustively which parties should provide information nor which information could be collected based on the provision, and the insured individual's right to self-determination would be reduced without reason. The DPA's observations were taken into account and the provision on data collection without consent was cancelled.

Organisation	Data Protection Authority
Chair and/or College	Sigrún Jóhannesdóttir, Commissioner, i.e. until April 2013 when Hörður Helgi Helgason became Commissioner; Björg Thorarensen, Chairman of the Board of Directors.
Budget	66 million ISK, i.e. around 415 800 € (according to the exchange rate on 31 December 2011)
Staff	Three legal counsels, one secretary

General Activity	
Decisions, opinions, recommendations	Ca. 120
Notifications	485
Prior checks	118
Requests from data subjects	510
Complaints from data subjects	90
Advice requested by parliament or government	Ca. 50
Other relevant general activity information	In total, 1 638 new cases were registered in 2013
Inspection Activities	
Inspections, investigations	0 (due to very limited resources because of financial cutbacks)
Sanction Activities	
Sanctions	With the exception of daily fines, imposed for each day that the DPA's orders are not obeyed, the DPA does not have sanction power.
Penalties	Daily fines were not imposed in 2013.
DPOs	
Figures on DPOs	N/A

B. Information on case-law

In May 2013, the board of the Icelandic DPA addressed an application for a processing permit from Decode Genetics (Íslensk erfðagreining in Icelandic), a company that analyses and researches the human genome, and the National Hospital (Landspítali). According to the application, the National Hospital was going to transmit extensive information to DeCode Genetics on everyone who had received service from the Hospital during a five-year period. Afterwards, DeCode Genetics would link the data with information it had previously collected, including genotype data, on individuals who had taken part in the company's other research projects, in total 95,085 individuals, without their consent. Furthermore, the data would be linked to estimates that DeCode had generated of the genotypes of 280,000 individuals who had not participated in the company's research projects, also without obtaining consent. The DPA considered this processing so extensive that it could only seek legal basis in the data subjects' consent or an act of law fulfilling strict constitutional conditions. Since neither prerequisite was fulfilled, the DPA refused to issue a permit. Furthermore, the DPA ordered Decode Genetics to delete the estimated genotypes of non-participants in its research projects.

In August 2013, the board of the Icelandic DPA made a ruling concerning a company called Já, which was founded in 2005 to manage the national phone registry and other information systems and - solutions. Já decided to publish on its website a system for presenting photographs of urban areas with a 360° view very similar to Google Street View. Já's presentation of the project entailed that the processing would not be personally identifiable. However Já's street view did publish identifiable photographs in which people's faces and the licence plates of cars were easily recognizable. The DPA considered this to be contrary to Act. No. 77/2000 and ruled that Já should render its photographs non-identifiable. Já later gave the DPA confirmation that it had blurred all identifiable photographs.



LIECHTENSTEIN

A. Summary of activities and news

In 2012, the Data Protection Office (DSS) defined the topics of health and welfare, Liechtenstein as a financial centre, and data security as the priorities for the coming years. These areas are very complex. International and European developments have to be followed in order to safeguard the private sphere. Overall, the role is and remains dynamic and challenging. The first steps towards implementing these priorities were taken in 2013. The need to define these priorities derives from the breadth of the topics being addressed on the one hand, and from the limited resources of the Data Protection Office on the other.

Education continues to represent the most important task for the DSS. This is based, in particular, on a representative survey by the DSS, which showed that the population still knows little about data protection. Following from the NSA scandal, the DSS has drawn up and published specific tips about how people can protect themselves. Alongside the traditional Data Protection Day, a podium discussion on the NSA scandal and the possible impact on Liechtenstein was organised with the association Verein Sicheres Liechtenstein. The DSS also held various training courses, with a focus on data security and secure communication on one hand and on educating young people and students in the use of new media on the other.

The availability of resources for the population and for individual target groups has also been expanded, e.g. with a guideline for processing personal data at work. This guideline discusses the legal situation and covers the entire range from application to job reference. It looks at various individual cases in practice, such as the use of social networks or “Bring your own device” in the workplace. A model data protection declaration has also been created, for example, for operators of internet sites, along with a recommendation on logging. These tools are available from the DSS website.⁷

Organisation	Data Protection Office
Chair and/or College	Philipp Mittelberger
Budget	EUR 596 000
Staff	2.3 Legal Affairs, 1.0 Technology, 0.8 Administration
General Activity	
Decisions, opinions, recommendations	10 Authorisations for video surveillance systems
Notifications	By the end of the year, a total of 308 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

⁷ <http://www.llv.li/#/1758/datenschutzstelle>

Requests from data subjects	98 Requests from private individuals
Complaints from data subjects	N/A
Advice requested by parliament or government	10 Responses to draft legislation
Other relevant general activity information	669 Requests (incl. from private individuals, see above)
Inspection Activities	
Inspections, investigations	6 Inspections completed
Sanction Activities	
Sanctions	N/A
Penalties	N/A
DPOs	111 Data protection officers
Figures on DPOs	

B. Information on case-law

No decisions by the Data Protection Commission were published in 2013.

NORWAY



A. Summary of activities and news

A strategic approach to counselling

It is strategically important for the DPA to be a key player early in any process, and we are pleased that government agencies, organizations, and businesses see us as an important interlocutor.

Privacy by Design.

In recent years, we have tried to promote the principles of Privacy by Design. This may include automatic deletion of data or automated audit solutions. In the White Paper Report to the Storting (Norwegian Parliament) "Privacy - prospects and challenges", it is established that the principles of Privacy by Design are to be used when developing government IT solutions. We are pleased with this view and aim to follow this work in the future.

The Snowden year

2013 was the year we learned of Edward Snowden. The DPA has actively participated in the debate that followed his revelations. There is hardly any limit to how far a state can go in monitoring its citizens. The technology's potential is unlimited and, from our side, it was important to point out that monitoring of this kind is not acceptable.

Welfare Technology

Welfare technology has been a focal point for the DPA in 2013 and will be in the future. New legislation allows the use of tracking technology on demented people, and with it, a change of focus from being about authority to using welfare technology to examine how these technologies can be utilized in the best way possible. Again, the principles of Privacy by Design can prove successful.

Meanwhile, welfare technology will challenge privacy. Many of the solutions we see today involve some sort of surveillance. Due to this fact, we lecture on a balance between the usefulness of the technology and privacy consequences. In addition, when used to reduce consequences as much as possible through consent, information, and adequate security, etc., we may strike the right balance.

Publication of the report "Big Data – privacy principles under distress"

The DPA completed a comprehensive report outlining the challenges for privacy when using Big Data. The report also provides advice on how to use Big Data and, at the same time, respect the privacy of individuals. In the report, we point out the following challenges:

- Use of data for new purposes
- Data Maximization
- Lack of transparency
- Assembly may provide sensitive information
- Good-Bye anonymity?
- Data - determinism
- Chilling effect

Following the initiative of the DPA, the Berlin Group decided to create a working paper on Big Data. The prepared draft was presented to the members of the Berlin group in September 2013, was very well received, and is expected to finally be approved at the group's next meeting in May 2014.

Organisation	Norwegian Data Protection Authority
Chair and/or College	Director Bjørn Erik Thon
Budget	37 mill NOK
Staff	41
General Activity	
Decisions, opinions, recommendations	N/A
Notifications	8 912 new registered, total active 15 979
Prior checks	155
Requests from data subjects	In total, the Norwegian DPA received 5 032 phone calls and 2 546 e-mails to our counselling service.
Complaints from data subjects	N/A
Advice requested by parliament or government	We received 134 invitations to comment on new legislation and sent in comments on 52 occasions.
Other relevant general activity information	
Inspection Activities	
Inspections, investigations	Workplace - 15 Health sector – 28 Justice and police – 5 Public Sector – 15 School and education – 10 Other - 3 Total - 76
Sanction Activities	
Sanctions	7 penalty fees, and no coercive fee, all by DPA
Penalties	Penalty fees total 1 925 000 NOK.
DPOs	

Figures on DPOs	210 DPOs representing a total of 420 firms and public offices.
-----------------	--

B. Information on case-law

Gjensidige Insurance - illegal assessment activities

In May 2013, the DPA conducted an audit of Gjensidige Insurance. The purpose was to check how they processed personal data, especially when conducting investigations to uncover fraud or attempted fraud. The audit revealed highly invasive methods in connection with the investigation. They used concealed observation and hidden audio and video surveillance to prove a person's health conditions. The audit also revealed major shortcomings in the company's internal procedures for handling personal information in general. We deemed the deficiencies to be so serious that there was an intolerable risk that the company would violate the Personal data act's other provisions. We ordered the company to pay 600,000 kroner as a violation penalty - the largest fee the DPA has imposed so far. The company was also required to establish internal procedures in accordance with the Personal Data Act.

C. Other important information

Proposal for a new act on health registers (for medical treatment) and medical journals (secondary purpose).

In 2013, the Ministry of Health and care services proposed a new law on health records and a new law on medical journals. The DPA supports the proposal to divide the regulation into two different acts, one for treatment-oriented health records and one for health records for management, administrative, and research purposes.

On the other hand, we had major concerns regarding the proposal i.e., in regard to the weakening of a patient's right to self-determination.

Chapter Five

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

MEMBERS OF THE ARTICLE 29 WORKING PARTY ON DATA PROTECTION IN 2013

Austria	Belgium
<p>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.dsk.gv.at/</p>	<p>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 2 274 48 00 Fax: +32 2 274 48 35 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/</p>
Bulgaria	Cyprus
<p>Mr Ventsislav Karadjov Commission for Personal Data Protection –CPDP (Комисия за защита на личните данни) 2 Prof. Tsvetan Lazarov Blvd. Sofia 1592 Tel. + 359 2 915 35 31 Fax: + 359 2 915 35 25 E-mail: kzld@cpdp.bg Website: http://www.cdpd.bg</p>	<p>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</p>
Czech Republic	Denmark
<p>Mr Igor Nemeč 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/</p>	<p>(Temp.) Mrs. Birgit Kleis Danish Data Protection Agency (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 København K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk</p>

Estonia	Finland
<p>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@laki.ee or international@aki.ee Website: http://www.aki.ee</p>	<p>Mr Reijo Aarnio Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) Ratapihantie 9, 6th floor - FIN – 00521 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</p>
France	Germany
<p>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: lfalquepierrotin@cnil.fr Website: http://www.cnil.fr</p>	<p>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</p> <p>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</p>

Greece	Hungary
<p>Mr Petros Christoforos Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athens Tel: +30 210 6475608 Fax: +30 210 6475789 E-mail: p.christoforos@dpa.gr Website: http://www.dpa.gr</p>	<p>Mr Attila Péterfalvi President of the National Authority for Data Protection and Freedom of Information Szilágyi Erzsébet fasor 22/C H-1125 Budapest Tel. +36 1 3911 400 E-mail: ugyfelszolgalat@naih.hu Website: http://www.naih.hu</p>
Ireland	Italy
<p>Mr Billy Hawkes Data Protection Commissioner (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlinton, IE -Co.Laois Tel: +353 57 868 4800 Fax:+353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie</p>	<p>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</p>
Latvia	Lithuania
<p>Mrs Signe Plumina Data State Inspectorate of Latvia (Datu valsts inspekcija) Blaumana street 11/13-15 Riga, LV-1011 Tel: + 371 67223131 E-mail: info@dvi.gov.lv Website: www.dvi.gov.lv</p>	<p>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</p>
Luxembourg	Malta
<p>Mr Gérard Lommel National Commission for Data Protection (Commission nationale pour la protection des données)</p>	<p>Mr Joseph Ebejer Information and Data Protection Commissioner Office of the Information and Data Protection</p>

<p>- 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</p>	<p>Commissioner 2, Airways House High Street Sliema SLM 1549 Tel: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Website: http://www.idpc.gov.mt</p>
The Netherlands	Poland
<p>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: www.cbpweb.nl / www.mijnprivacy.nl</p>	<p>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 73 12; +48 22 860 70 81 Fax: +48 22 860 73 13 E-mail: desiwm@giodo.gov.pl Website: http://www.giodo.gov.pl</p>
Portugal	Romania
<p>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</p>	<p>Mrs Ancuța Gianina Opre National Supervisory Authority for Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Gen. Gheorghe Magheru Bld. 28-30, 1st District, RO - Bucharest Tel: +40 31 805 9211 Fax: +40 31 805 9602 E-mail: anca.opre@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro</p>
Slovakia	Slovenia
<p>Mrs Eleonóra Kročianová Office for the Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej</p>	<p>Mrs Natasa Pirc Musar Information Commissioner (Informacijski pooblaščenec)</p>

republiky) Hraničná 12 - SK - 82007 Bratislava 27 Tel: +421 2 3231 3211 Fax: +421 2 3231 3234 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	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 Rodríguez 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: 0303 123 1113 (local rate) Tel: +44 1625 545745 (national rate) Fax: +44 1625 524510 E-mail: please use the online enquiry form on our website Website: http://www.ico.org.uk	Mr Peter Hustinx European Data Protection Supervisor - EDPS Postal address: Rue Wiertz, 60, BE - 1047 Brussels Office: Rue Montoyer, 30, BE - 1000 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

OBSERVERS OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY IN 2012

Iceland	Norway
<p>Mr Hörður Helgi Helgason Director 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</p>	<p>Kim Ellertsen Legal director Norwegian Data Protection authority (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</p>
Liechtenstein	Republic of Croatia
<p>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</p>	<p>Mrs. Dubravka Dolenc Deputy Director Mrs Sanja Silaj Zeman Head of Department for International Cooperation, European 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 sanja.silaj-zeman@azop.hr Website: http://www.azop.hr</p>
The former Yugoslav Republic of Macedonia	
<p>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</p>	

Secretariat of the Article 29 Working Party

Mrs Marie-Hélène Boulanger

Head of unit

European Commission

Directorate-General Justice

Data Protection Unit

Office: M059 02/13 - BE - 1049 Brussels

Tel: +32 2 295 12 87

Fax: +32 2 299 8094

E-mail: JUST-ARTICLE29WP-SEC@ec.europa.eu

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

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

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

Priced publications:

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

