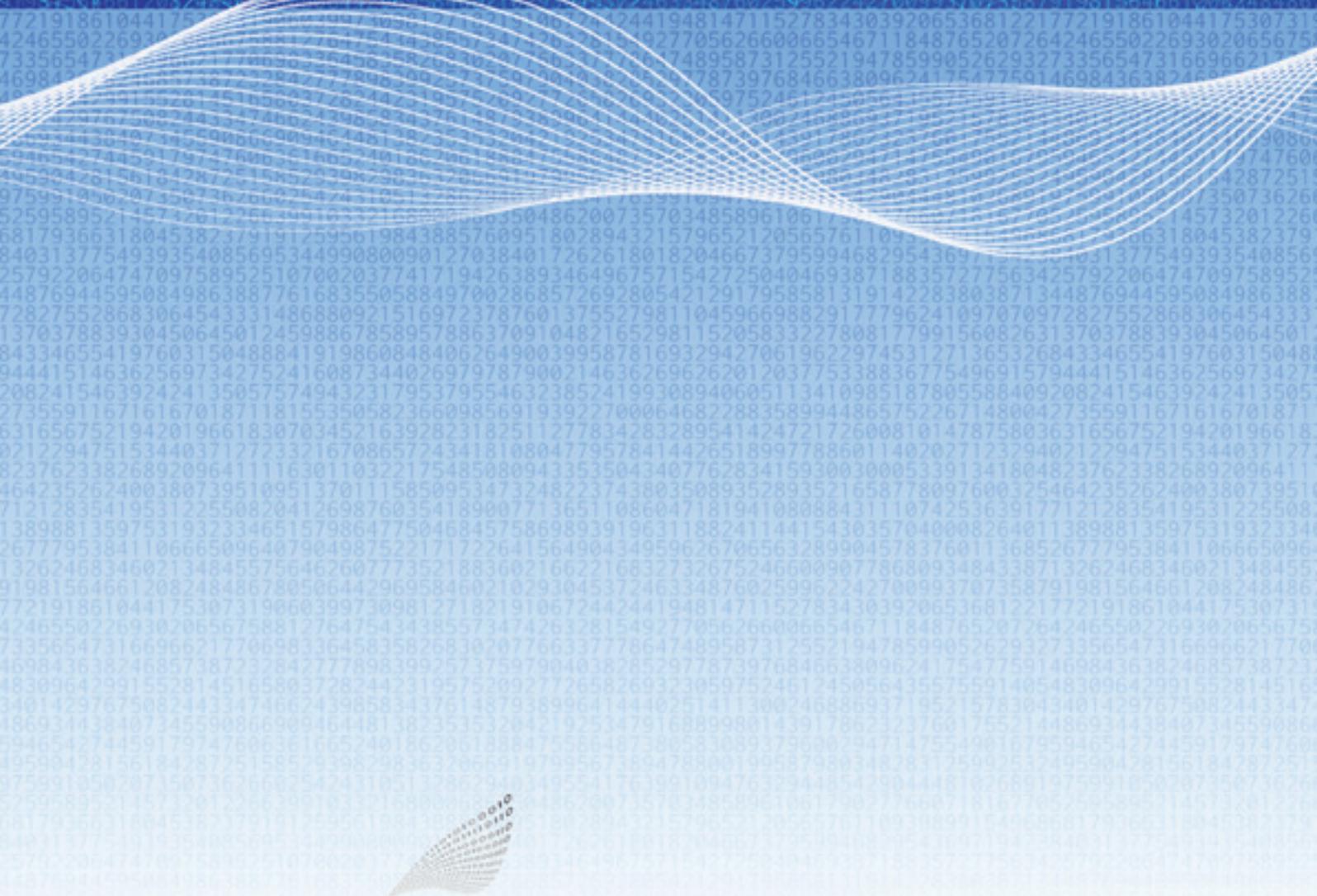


EUROPEAN DATA PROTECTION SUPERVISOR

ANNUAL REPORT 2014

EXECUTIVE SUMMARY



EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

ANNUAL REPORT 2014

EXECUTIVE SUMMARY

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

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

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

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

Luxembourg: Publications Office of the European Union, 2015

Print	ISBN 978-92-9242-059-8	ISSN 1831-0494	doi:10.2804/76098	QT-AB-15-001-EN-C
PDF	ISBN 978-92-9242-062-8	ISSN 1977-8333	doi:10.2804/10330	QT-AB-15-001-EN-N

© European Union, 2015
© Photos: EDPS & European Union

Reproduction is authorised provided the source is acknowledged.

Printed in Italy

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

INTRODUCTION

In recent years, data protection has moved from the margins to the centre ground of political decision making and business planning.

For the EU, 2014 may be remembered in future years as a watershed, the moment the rights to privacy and to the protection of personal data as set down in the Charter of Fundamental Rights moved decisively from legal theory to reality. The European Court of Justice, in its landmark judgments on the *Data Retention Directive* and *Google Spain*, articulated the responsibility of lawmakers and controllers for ensuring personal information is processed fairly and in a manner proportionate to the legitimate purpose being pursued. Deliberations on the reform of the EU's rulebook, which are now in their fourth year, edged closer to a conclusion, with the European Parliament giving a resounding endorsement to a revised text of the General Data Protection Regulation, and the Council grappling with the crucial questions of enforcement and consistency. Meanwhile, concerns about mass surveillance deepened, with the growing realisation of the need to revise and to clarify the parameters for data flows between the EU and its global partners.

2014 was a year of transition for the EU in general, as well as for our own institution. This Annual Report reviews the activities of the European Data Protection Supervisor and our focus on increasing the capacity of EU bodies for accountable data processing and for more proactive integration of data protection rules and principles in policy making. In addition to prior checks of processing operations and inspections, and numerous Opinions and comments on policy initiatives, including comments on the ongoing data protection reforms, we have published several key guidance documents addressing, for example, data subjects rights, data transfers and data protection in financial services regulation. This version of the EDPS Annual Report summarises the more detailed review of activities found in our full Annual Report.

This establishment of data protection in the mainstream of EU policymaking is a tribute to the calm authority and tireless efforts of Peter Hustinx, whose 10-year tenure as a European Data Protection Supervisor drew to a close in 2014, and to the talents and commitment of the people who work for this institution. Building on Peter's legacy, our priorities for the next five years, as set out in our Strategy published in March 2015, is to work more closely than ever with national data protection authorities as well as the Parliament and Member States, so that the EU speaks with one voice, credible and consistent, to uphold the rights and interests of the individual in our ever more globalised and digitalised society.



Giovanni Buttarelli
European Data Protection Supervisor



Wojciech Wiewiórowski
Assistant Supervisor

2014 HIGHLIGHTS

2014 was a year of transition for the EDPS, marked by the delayed selection and appointment of a new Supervisor and Assistant EDPS. The nominations that had been expected at the beginning of the year took place only at the end. While the resulting uncertainty had an impact on the planning of activities of the EDPS as a whole, we continued to perform our duties in line with our obligations under [Regulation \(EC\) 45/2001](#).

Supervision & Enforcement

As in previous years, an important part of our workload was composed of core supervision and enforcement activities over the processing of personal data by over 60 European institutions and agencies. Prior checks, consultations, complaints, inspections and visits accounted for the central part of our work in that domain. With relatively high numbers of cases, we nevertheless managed to improve the efficiency of our workflow.

In addition, in close cooperation with the data protection officers appointed in each EU institution and body, we continued to invest in awareness raising and guidance throughout the year to help promote a data protection culture in the EU institutions. Of particular note were:

- Rights of Individuals (Data Subjects Rights) [Guidelines](#) adopted in February,
- the Data Transfer [Position Paper](#) adopted in July and
- the Conflicts of Interest [Guidelines](#) adopted in December;
- several meetings with controllers to address specific data protection issues of the EU administration;
- three conferences at the European School of Administration (EUSA) and one workshop for Data Protection Coordinators;
- two DPO meetings in June and November.

More proactive policy advice

In 2014, we reviewed how we fulfil our legal obligation to advise the institutions. In our June [policy paper](#), 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience'¹, we reiterated our principles of impartiality, integrity, transparency and pragmatism and our broad, inclusive and proactive engagement with stakeholders. We aim to develop a culture of accountability across all institutions and EU bodies through training and general as well as sector specific guidance to enable the institutions to make informed decisions on the data protection impacts of new proposals. We have already begun to target engagement with less familiar interlocutors including the Commission's internal market and services directorate general (DG MARKT) and the Council presidency who are increasingly aware of the relevance of data protection. In addition, we have established regular liaison and information sharing with the Fundamental Rights Agency (FRA) and international bodies including the Council of Europe.

We launched an analysis of the interaction between data protection, competition and consumer law by publishing a preliminary Opinion on [Privacy and competitiveness in the age of big data](#) in March 2014. A discussion on the subject was launched at a workshop in June 2014 with the participation of experts in all three areas of law from the EU and the USA.

On the basis of constructive and targeted dialogue with the institutions, we specifically undertook to develop a 'policy toolkit' – including thematic or sectoral guidelines – for guiding policy and law makers on the relevance of the fundamental rights to privacy and to data protection in specific sectors.

In November 2014, we delivered the first of these tools focusing on financial services regulation, an area of intense legislative reform in recent years. Our sector guidelines built on insights gained during a seminar hosted by DG MARKT in February 2014.

¹ EDPS Policy Paper, 'The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience', 4 June 2014.

Towards a new legal framework for data protection: An end in sight?

Reforming the data protection framework has constituted one of the largest and most complex challenges for EU lawmakers in recent years. There is great interest at national, European and international level in the evolution of the two draft proposals - for a General Data Protection Regulation and a Directive on personal data processed for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The EDPS continued to work closely with the Parliament, the Council and the Commission during the critical negotiations which took place in 2014.

Cooperation

In 2014 as in 2013, we provided the secretariat for the new Schengen Information System II (SIS II) Supervision Coordination Group and we chaired the supervision coordination groups for EURODAC, Visa Information System (VIS) and the Customs Information System (CIS).

We also continued to contribute actively to the work of the Article 29 Data Protection Working Party (Article 29 Working Party), acting as rapporteur for the follow-up of the Opinion on Legitimate Interests (consultation of stakeholders and analysis of their contributions), and co-rapporteurs for the Opinion and the Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes, as well as for the paper on the International Enforcement Coordination Arrangement.

Technological development and data protection

The impact of the wider spread of connected mobile devices and a high number of security incidents were among the themes of 2014 and we reported on these and other technological developments in the EDPS [newsletters](#).

We also addressed technological elements in our policy Opinions and comments and decisions in the supervision domain, as well as in guidelines, e.g. the e-communications guidelines, which were distributed for consultation in 2014.

In 2014, we set up the EDPS IT Policy Laboratory with equipment and tools that can be used to assess the privacy features of certain products or systems used in the field of our supervision work.

The IT lab is now operational and will be complemented by a mobile IT kit, in order to provide on-the-spot demonstrations, perform experiments and/or technical tests on site in the context of inspections and audits.

We also turned our focus on data protection and privacy from an engineering perspective. In 2014, we launched the Internet Privacy Engineering Network (IPEN) in collaboration with national data protection authorities, developers and researchers from industry and academia and civil society. The initiative aims to develop engineering practices which incorporate privacy concerns and encourage engineers to build privacy mechanisms into internet standards, services and apps.

The first IPEN [workshop](#) took place on 26 September 2014 in Berlin and was organised together with several DPAs and other organisations. The workshop was designed to be a practical approach to identify privacy gaps in existing technology and develop useful solutions. In 2015, the network will expand and continue to work on lines of action established in 2014.

Court Cases

With regard to Court activities we were granted leave to intervene by the Court of Justice and submitted a written statement in an appeal Case C-615/13 P, brought by ClientEarth and PAN Europe), a case related to transparency/access to documents.

Information & Communication

Information and communication activities play a significant role in raising awareness of the EDPS, the mandate, policies and decisions.

In 2014, we promoted the work of the EDPS at a number of events, such as Data Protection Day in January, the EU Open Day in May and four lunch time conferences at the European School of Administration (EUSA).

Within the scope of our competence, we replied to 132 written information requests from citizens,

38 written information requests and 42 interview requests from the press.

By the end of 2014, we had 2373 subscribers to our newsletter and 2000 Twitter followers. We had 194,637 visits to the EDPS website and we hosted seven study visits on our premises. These achievements all support the view that we are increasingly a point of reference for data protection issues at EU level.

Resource Management

The allocated budget for the EDPS in 2014 was EUR 8 018 796, which is an increase of 4.66% on the 2013 budget.

In 2014, we remained fully committed to the EU's policy of austerity and budget consolidation, and followed the orientations proposed by the Commission strictly. Nevertheless, our budget proposal had to include the necessary appropriations to comply with the statutory obligations linked to the end of mandate of the members of the EDPS.

We implemented the austerity policy recommended by the Commission by reducing or freezing a large majority of our credits to 0% for the third year and carrying out substantial cuts to key budget lines such as translations (-17%), publications (-25%) and activities of the institutions (-17%).

The delay in the selection procedure for a new team of Supervisors has led to the introduction of an amending budget to return the unused credits linked to temporary extension of the mandate to the general EU budget in June 2014.

In 2014, the implementation rate of our budget exceeded the target of 85%.

2014 was a particularly successful year in the human resources area. On the one hand the entry into force of the new Staff Regulations in January 2014 required many implementing measures to be updated. The full package of implementing rules was adopted before the end of the year.

On the other hand a number of important policy documents were also adopted, notably the new Learning and Development policy and its implementation, two pilot projects and the papers on DNA, Stress and Internal Communication. Finally, a new Code of Conduct for EDPS Staff was adopted and presented to the Staff.

Key EDPS figures in 2014

- 144 prior-check Opinions adopted, 26 non-prior check Opinions
- 110 complaints received, 39 admissible
- 48 consultations received on administrative measures
- 4 on-the-spot inspections and 4 visits carried out
- 2 sets of Guidelines published, 1 Position Paper
- 14 legislative Opinions and 1 Preliminary Opinion issued
- 13 sets of formal comments issued
- 33 sets of informal comments issued

Strategy 2013-2014

In our Strategy 2013-2014, we identified a number of strategic objectives to help increase the impact of our core activities on data protection at European level. To assess our progress towards these objectives, we identified the activities which play a key role in achieving our goals. The related key performance indicators (KPIs) listed in the table help us to monitor and adjust, if needed, the impact of our work and the efficiency of our use of resources.

In this chapter, we report on the performance of our activities in 2014 in accordance with the strategic objectives and action plan defined in the Strategy 2013-2014. The activities implementing the action plan are summarised in the General Overview of 2014, above.

Overall, the results show a positive trend in the performance of our activities. The implementation of the strategy is broadly on track and no corrective measures are needed at this stage.

In addition, the adoption of the Strategy 2015-2019 in March 2015 will require an evaluation of the KPIs to take into account the objectives and priorities

of the new Strategy. As a result, to ensure their consistency and relevance, there may be one or more new KPIs, which will be submitted to thorough internal consultation before being published.

The KPI scoreboard contains a brief description of the KPIs and the methods of calculation.

The indicators are measured against initial targets in most cases. For three indicators, the results of 2013 set the benchmark for 2014.

The KPIs implement the strategic objectives as follows:

1. Promote a *data protection culture* within the EU institutions and bodies whereby they are aware of their obligations and accountable for compliance with data protection requirements.
KPIs numbers 1, 2 and 3. All targets have been achieved.
2. Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and that data protection is integrated in new legislation.
KPIs numbers 4 and 5. The target for KPI number 5 has been achieved. The results for KPI number 4 are in line with 2013 results with regard to formal and informal comments, while the number of opinions decreased in 2014. This was due, on the one hand, to a greater level of selectiveness and on the other to the fact that several Commission
3. Improve the good cooperation with data protection authorities (DPAs), in particular the WP29, to ensure greater consistency of data protection in the EU.
The results of 2013 determine the target for KPI number 6. The results in 2014 were a great success, as they largely exceeded the target.
KPI number 7 refers to strategic objectives 1, 2 and 3. The target was largely exceeded.
4. Develop an effective communication strategy.
The results of 2013 determine the target for KPI number 8. In this respect the number of visits to the EDPS website decreased during 2014. The main reason was the delayed appointment of the new Supervisors. During the one-year extension of the mandate there were fewer new decisions or new projects. This had an impact on the interest to visit our website.
5. Improve the use of the EDPS' human, financial, technical and organisational resources (through adequate processes, authority and knowledge).
KPIs numbers 9 and 10. Both targets have been achieved.

KPIs	Description	Results 2013	Results 2014	Target
KPI 1	Number of inspections/visits carried out Measurement: compared to target	3 visits 8 inspections	4 visits 4 inspections	8 minimum
KPI 2	Number of awareness-raising and training initiatives within EU institutions and bodies which we have organised or co-organised (workshops, meetings, conferences, training and seminars). Measurement: compared to target	4 trainings 4 workshop (3 in cooperation with ITP)	8 (3 EUSA, 1 DPC, 2 DPO, 1 EIPA, 1 DG COMM)	8 (workshops + trainings)
KPI 3	Level of satisfaction of DPOs/DPCs on training and guidance. Measurement: DPOs/DPCs satisfaction survey to be launched every time a training is organised or a guidance is issued	DPO basic training: 70% positive feedback EDA staff training: 92% positive feedback	100%	60% positive feedback
KPI 4	Number of EDPS formal and informal Opinions provided to the legislator. Measurement: compared to previous year	Opinions: 20 Formal comments: 13 Informal comments: 33	Opinions: 15 Formal comments: 13 Informal comments: 33	2013 as benchmark
KPI 5	Rate of implementation of cases in our policy inventory which we have identified for action. Measurement: percentage of 'Red' initiatives (where the dead-line for comments has expired) implemented as planned in the Inventory 2013	90% (18/20)	89%	90%
KPI 6	Number of cases dealt with by the Article 29 Working Party for which the EDPS has provided a substantial written contribution. Measurement: compared to previous year	13	27	2013 as benchmark
KPI 7	Number of cases in which guidance is provided on technological developments. Measurement: compared to target	21	58	20
KPI 8	Number of visits to the EDPS website. Measurement: compared to previous year	293.029 (+63% in comparison to 2012)	194.637	2013 as benchmark
KPI 9	Rate of budget implementation Measurement: amount of payments processed during the year divided by the budget of the year.	84,7%	85,8%	85%
KPI 10	Rate of training implementation for EDPS staff Measurement: number of actual training days divided by the number of estimated training days	85%	87,4%	80%

SUPERVISION AND ENFORCEMENT

One of the main roles of the EDPS is to supervise in an independent manner, the processing operations carried out by European institutions or bodies. The legal framework is the Data Protection Regulation (EC) No 45/2001, which establishes a number of obligations for those who process data, along with a number of rights for those whose personal data are processed.

Supervisory tasks range from advising and supporting data protection officers through prior checking of risky data processing operations, to conducting inquiries, including on-the-spot inspections and handling complaints. Further advice to the EU administration can be provided in consultations on administrative measures or the publication of thematic guidelines.

Our strategic objective

Promote a 'data protection culture' within the EU institutions and bodies so that they are aware of their obligations and accountable for compliance with data protection requirements

Data Protection Officers

In 2014, we received notifications for the appointment of 9 new data protection officers (DPOs) in the EU institutions.

We attended the DPOs meeting held in Brussels in June (hosted by the European Parliament and the European Commission) and in Thessaloniki (hosted by the European Centre for the Development of Vocational Training, CEDEFOP) in November.

At the June meeting, we presented an update on the EU reform of the data protection legislation and relevant case law in the area. The meeting was also an appropriate opportunity for us to present our guidelines on data subject rights which led to an in-depth discussion on how to address such requests in practice.

The meeting at CEDEFOP was an occasion to reflect on the new EDPS mandate and the role of DPOs in the international scene. We also presented our

position paper on transfers which was adopted in July 2014 and our guidelines on conflicts of interests, both of which gave rise to interesting debates. Also well appreciated was our update on security and technology issues with particular reference to the EDPS experience of using the cloud and security breach handling. We also presented some notable issues dealt with in our Supervision and Enforcement work such as the procedure for consultations at the CCA (Collège des Chefs d'administration), the involvement of DPOs in complaint handling and the importance of documenting deferral of rights in accordance with Article 20 of the Regulation.

In June 2014, we organised a training session for DPOs back-to-back with the DPOs meeting. In addition, one-to-one sessions took place between EDPS staff and some DPOs on their specific guidance needs. The development of consultancy visits has also served to address the specific needs of DPOs.

In response to the increasing number of telephone queries we receive, we set up a helpline for DPOs, operational at set times in the week and answered by an EDPS member of staff. The helpline allows us to provide specific guidance on simple questions from DPOs in a quick and informal way and strengthens the good cooperation and communication between us and the DPO community within the EU institutions. In 2014, the helpline averaged around 4 calls per month.

Prior checking

A large number (80% in 2014) of the risky processing operations notified to us relate to administrative procedures common to all EU institutions and bodies, such as the recruitment of staff, their annual evaluation or the conduct of administrative inquiries.

As we received a significant number of notifications in 2013 and 2014 and an even larger number of recommendations to be followed, we developed a criteria to help us be more selective about the recommendations we follow up. This selectivity allows us to concentrate our efforts on managing

risky processing operations. Our other recommendations are followed up by the DPO of the relevant institution or body, in line with the principle of accountability.

The prior checking exercise provides a systematic way of learning about the activities of the EU institutions and bodies and allows the EDPS to understand patterns or shortcomings in the implementation of data protection principles. The prior checking activity is a matrix of knowledge for us; the high number of Opinions issued helps to build other supervisory tools such as inspections, surveys, inquiries, compliance and consultancy visits.

In 2014, we received 80 notifications for prior checking with one subsequently withdrawn. Progress continued to be made in clearing the back-log of *ex-post* notifications received in 2013.

In 2014, we issued 144 prior check Opinions (an increase of approximately 58% from 2013) and 26 Opinions (a 24% increase from 2013) on 'non prior checks'². In total, we examined 185 notifications, some of which led to joint Opinions. A variety of issues were analysed, some of which are reported in the full version of this report.

Complaints

One of the main duties of the EDPS, as established by Regulation (EC) No 45/2001, is to 'hear and investigate complaints' as well as 'to conduct inquiries either on his or her own initiative or on the basis of a complaint' (Article 46).

In 2014, the EDPS received 110 complaints, an increase of approximately 41% compared to 2013. Of these, 72 complaints were inadmissible, the majority relating to processing at national level as opposed to processing by an EU institution or body.

The remaining 39 complaints required in-depth inquiry, an increase of about 30% compared to 2013. In addition, 18 admissible complaints, submitted in previous years (three in 2011, three in 2012 and 12 in 2013), were still in the inquiry, review or follow-up phase on 31 December 2014.

² When a notification is received by the EDPS, but the processing operation does not fall within the scope of Article 27, the EDPS may nevertheless issue recommendations.

Monitoring compliance

The EDPS is responsible for monitoring and ensuring the application of Regulation (EC) No 45/2001. This monitoring is performed in several ways: by bi-annual periodic general surveys or more targeted monitoring exercises such as a visit or inspection.

We have recently developed a new type of on-site visit called **consultancy visits** where two members of EDPS staff are nominated as on-site consultants. This type of visit is a practical tool to tackle specific problems, raise awareness, improve cooperation and enhance the accountability of the targeted body. In one instance, we followed-up a consultancy visit with a short **secondment** of an EDPS member of staff.

Between January and December 2014, we visited four EU agencies: the European Investment Fund, the EU Satellite Centre, the GNSS Supervisory Authority and the EU Institute for Security Studies.

In 2014, we continued the follow-up of previous inspections. In addition, we inspected Frontex, the European Parliament and conducted a targeted inspection on health data at the European Commission and the Council.

Consultations on administrative measures

The EDPS issues Opinions on data protection matters, following a request either from an EU institution or on his own initiative. The EDPS may give an opinion on a decision or any other act of the administration of **general application** relating to the processing of personal data carried out by the EU institution concerned (Article 28(1)). The EDPS may also give advice on cases involving **specific processing activities or questions** on the interpretation of the Regulation (Article 46(d)).

The principle of **accountability** applies to the management of consultations. EU institutions should first seek the internal advice of their DPO and therefore involve their DPO when drawing up measures affecting the right to data protection. If the DPO is not in a position to provide an appropriate solution, the EDPS can be consulted. The consultation must relate to **new** or **complex issues** (no precedent in the field, lack of doctrine or lack of clarity in the definition of certain concepts of the Regulation).

In 2014, we received 48 consultations on administrative measures. A variety of issues were examined, some of which are reported in the full version of this report.

Data protection guidance

In February 2014, we published **guidelines on the Rights of Individuals with regard to the Processing of Personal Data**.

The content of the guidelines is based on EDPS positions in the area of data subjects' rights, as developed in a series of EDPS Opinions on EU data processing operations. The guidelines describe our positions and recommendations on the relevant principles of Regulation 45/2001 and provide information on current best practice and other pertinent issues. For example, they highlight the broad concept of personal data under the Regulation, according to which personal data refers to much more than just the name of a particular individual.

On 14 July 2014, we adopted a **position paper on transfers** designed to provide guidance to EU institutions and bodies on how to interpret and apply the rules laid down in Regulation (EC) No 45/2001, when transferring personal data internationally.

Our guidance focuses mainly on the methodological analysis that EU institutions and bodies have to conduct before transferring personal information to third countries or international organisations.

Examples are given to facilitate the task of data controllers and data protection officers (DPOs) in applying these rules, as well as a checklist with the steps to be followed when applying Article 9 of Regulation 45/2001. The paper also provides the relevant information on the supervisory and enforcement roles of the EDPS within the context of data transfers.

In December 2014, we published **guidelines on the collection, processing and publication of personal data with regard to declarations**

relating to the management of conflicts of interest in EU institutions and bodies. The guidelines provide EU institutions and bodies with practical guidance on respecting the data protection rules and finding a balance between the public interest for transparency and the individual's rights to privacy and data protection. This balancing exercise can strengthen the efforts of institutions to foster the trust of the public as well as those who work for them.

As part of the process of making EU institutions more accountable, we are keen on providing **training and guidance** for DPOs, DPCs and controllers so that they may better understand the data protection principles and their possible obligations.

On 28 January 2014, EU data protection day, we participated in a DPC meeting at the European Commission, delivering a speech on the Regulation (EC) 45/2001 in the light of the current reform of the general data protection framework. This was an occasion to reflect with the DPCs on the specificities of the Regulation as an instrument for EU public service and possible improvements that would be welcome in the revision of the instrument.

On 13 June 2014, we organised a general training for DPOs from EU institutions and bodies with a focus on how to complete a notification form.

We also provided specific training sessions to staff of some agencies (FRONTEX) or their DPOs (ECDC, EUISS, EIF) on a request basis and one to trainees of the Council, Committee of the Regions and the Economic and Social Committee.

In June and December 2014, we gave presentations at training courses organised by the European Institute for Public Administration (EIPA) in Maastricht, which was attended by DPOs, DPCs and controllers. We spoke about the specificities of Regulation (EC) 45/2001, the role of the EDPS in the context of our Supervision and Enforcement work and presented two case studies, one on international transfers of personal data and the other one on the right of access in the context of a complaint.

POLICY AND CONSULTATION

The EDPS advises the European Union institutions and bodies on data protection issues in a range of policy areas. This consultative role relates to proposals for new legislation as well as other initiatives that may affect personal data protection in the EU. It usually takes the shape of a formal opinion, but the EDPS may also provide guidance in the form of comments or policy papers.

Our strategic objective

Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and integrates data protection in new legislation

2014 Priorities

With regard to specific initiatives, our 2014 'inventory' anticipated five key areas of strategic importance for data protection. Our work under these headings is summarised below (with more detail in the full report).

- Towards a new legal framework for data protection
- Rebuilding trust in global data flows in the aftermath of PRISM
- Initiatives to boost economic growth and the Digital Agenda
- Further developing the area of freedom, security and justice
- Reform of the financial sector.

Towards a new legal framework for data protection: An end in sight?

Reforming the data protection framework has constituted one of the largest and most complex challenges for EU lawmakers in recent years. There is great interest at national, European and international level in the evolution of the two draft proposals - for a General Data Protection Regulation, and for a Directive on personal data processed for

the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The EDPS continued to work closely with the Parliament, the Council and the Commission during the critical negotiations which took place in 2014.

Rebuilding trust in global data flows in the aftermath of PRISM

The mass surveillance of EU citizens by intelligence agencies and law enforcement agencies which was revealed in 2013 clearly flouted individuals' rights to privacy and to the protection of personal data. The EDPS addressed the public hearing of the European Parliament's Civil Liberties Committee in October 2013, emphasising serious concerns and the need for the EU to assert control of our privacy. We developed this message in our Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows'. We expressed support for a privacy act in the United States, and called for the promotion of international privacy standards alongside the swift adoption of reforms to the EU data protection framework.

Initiatives to bolster economic growth and the Digital Agenda

The EDPS has engaged constructively on a broad range of policy developments as varied as competitiveness and consumer protection, internet governance, the functioning of the internal market, the single digital market, and customs and agriculture. We have also closely monitored the developments concerning the Safe Harbour agreement, and the Commission negotiations of new trade agreements (eg TTIP, TISA) as regards their potential impact on privacy and data protection.

Further developing the Area of Freedom, Security and Justice

In 2014, as well as considering a number of specific initiatives, such as the future of Europol, Eurojust and the creation of a public prosecutor's office, gun control and asset freezing, the EU took stock

of its progress towards the creation of an area of freedom, security and justice. We continued to be active in shaping this broad agenda.

Reform of the financial sector

The EDPS has been developing its expertise in how to apply data protection standards in the design

and implementation of financial services regulation. We have issued our first set of guidelines for the sector, and provided advice on specific proposed measures in the areas of shareholder rights, resilience of the banking system and transparency in securities financial transactions.

COOPERATION

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.

Our strategic objective

Improve the good cooperation with Data Protection Authorities, in particular the Article 29 Working Party, to ensure greater consistency of data protection in the EU

In 2014, we continued to contribute actively to the activities of the **Article 29 Working Party** in order to ensure greater consistency of data protection in the EU.

As a member, the EDPS contributes to the activities of the working party taking up a share of the work, comparable to the one taken up by larger DPAs. However, this participation is based on a selective approach and focus where our contribution provides an added value, in particular in bringing an EU perspective, such as in the Working Party opinion on legitimate interest, or the opinion on open data. We were also closely involved in the opinions on device-fingerprinting and drones and on the internet of things.

Direct cooperation with national authorities is an area of increasing importance in the context of the development of large-scale international databases such as EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) or the Customs Information System (CIS), which require a coordinated approach to supervision. This cooperation work is in addition, but separate to our supervision work in this area (see chapter 2). In 2014 as in 2013, we provided the secretariat for the new SIS II Supervision Coordination Group and we chaired the supervision coordination groups for EURODAC, VIS and the CIS. Our role has included:

- appropriate planning for the timely allocation of financial and human resources;
- coordinating the meetings of the groups;
- drafting and circulating relevant documents;

- liaison with members of the groups in between meetings to prepare business.

On 5 June 2014, the EDPS attended the **European Conference of Data Protection Authorities** in Strasbourg, jointly organised by the Council of Europe and the French 'Commission Nationale de l' Informatique et des Libertés' (CNIL).

The 2014 conference focused on ways for DPAs to cooperate better in the face of globalisation. A resolution was adopted which called on the Council of Europe, in its ongoing deliberations on modernising Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, to strengthen protection of individual rights, in particular through establishing independent supervisory authorities which are able to enforce and to cooperate with each other effectively.

The 2014 **International Conference** was organised by the Data Protection Office of Mauritius from 12 October to 16 October.

Several themes were on the agenda including, privacy and data protection in the developing world; One Stop Shop: Centralisation versus Proximity; Surveillance versus Dataveillance; Privacy in the Digital Age – the UN General Assembly Resolution; E-Health and Data Protection; Ethics, Fundamental Rights and Big Data; and Net Neutrality and Data Protection. The Supervisor intervened in a workshop on accountability and a panel on 'privacy without territorial limits', and the Director spoke in a panel on net neutrality.

An important achievement of this conference was the adoption, in the closed session for data protection authorities (13-14 October), of the [Arrangement and Resolution on international enforcement cooperation](#). This project has been under discussion for many years and we have been very involved in supporting the negotiations. The rapid development of technologies such as cloud computing, big data and the internet of things (IOT) have underlined the need for a framework to enable data protection authorities to cooperate across borders.

The supervisor also gave a short presentation at the closed session on the IPEN initiative, which provoked great interest.

We also continued to attend key meetings or provide input on relevant documents discussed in the Council of Europe (Consultative Committees of Convention 108 and the Cybercrime Convention), the OECD, APEC, GPEN, the French-speaking association of personal data protection Authorities (AFAPDP), the Ibero-American data protection network, the international working group on data Protection in Telecommunications (Berlin Group) and

the international conference of data protection and privacy commissioners.

We also try to monitor, provide advice and comments where necessary and possible, on data protection developments in non-EU countries and privacy policies in international organisations, such as UNHCR.

COURT CASES

The right of the EDPS to intervene in actions before the court was recognised by the CJEU in the PNR cases (Cases C-317/04 and C-318/04, orders of 17 March 2005). The court based the right to intervene on the second subparagraph of Article 41(2) of Regulation (EC) No 45/2001 according to which the Supervisor is 'responsible for advising Community institutions and bodies on all matters concerning the processing of personal data'. This advisory task does not only cover the processing of personal data by those institutions or organs. The court interpreted the powers conferred on the EDPS by Article 47 of the Regulation in light of the purposes of Article 41.

In 2014, the EDPS intervened in several cases before the court:

- T-115/13 Dennekamp v Parliament (transparency/access to documents)

- T-343/13 CN v Parliament (publication of sensitive personal data on a website)
- C-615/13 P ClientEarth/PAN Europe (interpretation of the concept of personal data in the transparency/access to documents context and compliance with Article 8(b) of Regulation 45/2001, as well as the difference between the fundamental right to privacy and the fundamental right to personal data protection)

Under Regulation (EC) No 45/2001, actions against the EDPS can be brought before the CJEU (Article 32). For instance, EDPS decisions in complaint cases can be appealed before the CJEU. To date, three complainants have brought cases to court. The three cases were unsuccessful.

ACCESS TO DOCUMENTS/ TRANSPARENCY

As an EU institution and according to its Rules of Procedure, the EDPS is also subject to the Public Access to Documents Regulation of 2001. The number of public access requests for documents held by the EDPS has increased progressively over the years. The number doubled in 2013 from 12 requests to 24. In 2014, we dealt with 18 requests, 4 of which were confirmatory applications to our initial replies.

The increasing number of cases we deal with in this field reveals the need for more detailed guidelines on the practical implementation of the Public Access Regulation. We are currently working on consolidating the methodology on how to deal with replies, according to the latest practice. In 2015, we will provide practical advice to the EU institutions and bodies on how to balance transparency and the need for the protection of personal data in light of the Bavarian Lager ruling of the Court of Justice.

MONITORING TECHNOLOGY

In 2014, we continued to assess the privacy risks of new technologies by collecting and analysing information as appropriate. We also provided guidance on technical aspects of data protection compliance to controllers in a number of ways. A summary of some of this work follows but more information can be found in the full version of this report as well as in EDPS [newsletters](#).

More and more devices (for example, wearable or in car ones) are equipped with interfaces that allow transmission of the data they collect.

There are concerns that security might not be keeping up with the increased collection and transmission of personal data. The number of serious security flaws discovered in widespread systems is also increasing: in 2014, it was found that some of the most popular mobile devices were vulnerable to interception of seemingly encrypted communications. It was also revealed that a piece of code found in many Linux systems had a flaw allowing attackers to bypass security protections. A vulnerability was also discovered in smartphone operating systems where the chip responsible for the communication over the network could override all restrictions protecting the 'smart' part of the phone, and so gain access to all information stored on the smartphone.

In 2014, a number of security flaws in widely used systems found broad interest. Some of the vulnerabilities were given names like Heartbleed, Gotofail and Poodle. The Heartbleed bug³ was discovered in OpenSSL, a popular encryption tool for internet communications. Heartbleed makes it possible to read and access data that should be protected.

Many popular internet services seemed to be vulnerable and appeared to take the necessary measures to quickly fix the bug on their systems. The European institutions also secured their services. Users of affected services were advised to change their passwords and the certificates used for encrypting internet traffic between affected websites were replaced. Yet despite all these measures, it is possible that there are servers which have not yet been updated and which are therefore still using the affected software.

The EDPS IT Policy Laboratory was set up in 2014 with equipment and tools that can be used to assess the privacy features of certain products or systems used in the field of our supervision work.

The IT lab is now operational and will be complemented by a mobile IT kit, in order to provide on-the-spot demonstrations, perform experiments and/or technical tests on site in the context of inspections and audits.

In 2014, we launched the Internet Privacy Engineering Network (IPEN) in collaboration with national data protection authorities (DPAs), developers and researchers from industry and academia and civil society. The initiative aims to develop engineering practices which incorporate privacy concerns and encourage engineers to build privacy mechanisms into internet standards, services and apps.

The first IPEN [workshop](#) which took place on 26 September 2014 in Berlin was designed to be a practical approach to identify privacy gaps in existing technology and develop useful solutions.

Following the success of the first workshop, the IPEN initiative is now focused on developing and addressing the identified projects. IPEN will continue to explore ways to develop privacy-friendly technologies and to ensure that privacy becomes an essential consideration for all IT developers.

In November 2014, in line with providing advice to the EU legislator, we gave an overview of the applicable EU framework for data protection, as well as relevant elements of the reform at the European Commission's working group on Governance and Privacy at which discussions on the deployment of cooperative intelligent transport systems (C-ITS) took place. Privacy aspects are highly important to the deployment of C-ITS because the data could be used for profiling or tracking. We will continue to follow this initiative in 2015.

To further build on our capacity to give advice to controllers on technical measures for the effective implementation of data protection in IT systems, we have been developing guidelines for specific IT areas. The guidelines will be available in the course of 2015.

3 CVE-2014-0160.

In 2012, we were made aware of the systematic blocking by some EU websites of all access from the [Tor network](#). While network security concerns were given as justification for this restrictive measure, we pointed out that the EU regulatory framework explicitly recognises anonymous communications, and that necessity and proportionality would need to be assessed properly. Following these exchanges the relevant security policy was reviewed and Tor is no longer systematically blocked, to the benefit of European and non-European citizens which want or need to protect their web browsing privacy.

Our technology and IT policy expertise plays a valuable role in the EPDS' task of cooperating with other DPAs. In 2014, we participated in several

working group, task force or sub-group meetings. We also visited eu-LISA in Tallinn, the European agency for the operational management of large-scale IT Systems in the Area of Freedom, Security and Justice, in order to raise awareness on data protection-related matters and initiate discussions on IT and IT security management of the systems. This was independent of the inspection that we began of eu-LISA's Strasbourg site towards the end of 2014 in order to check the security and the operational management of the system

Among other things, we also contributed to the Commission's efforts in smart meters and grids policy and in its development of an approach for the use of cloud computing in public administration.

MAIN OBJECTIVES FOR 2015

The following objectives have been selected for 2015 within the overall Strategy for 2015-2019. The results will be reported in 2016.

Supervision and enforcement

In 2015, we will continue to promote the accountability of EU bodies when they process personal data.

- **Library of experience**
Utilising our ten years of experience in applying Regulation 45/2001, we will develop an internal repository of our case law to ensure that our valuable expertise is catalogued;
- **Regulation 45/2001**
Relying on this solid experience, we will work with the European Parliament, Council and Commission to ensure that the existing rules set out in Regulation 45/2001 are brought into line with the General Data Protection Regulation.
- **Training & interaction**
We will continue to train and guide EU bodies on how best to respect data protection rules in practice, focusing our efforts on those types of processing which present high risks to individuals. We will maintain our close interaction with EU bodies, offering them relevant expertise and advice, which in turn will help us to strengthen our practical knowledge of their reality.
- **DPOs**
In close cooperation with data protection officers, we will continue to support EU institutions in moving beyond a purely compliance-based approach to one that is also based on accountability. In particular, we will work with them to develop data privacy impact assessments and data breach notifications.
- **Coordinated Supervision**
We will continue to supervise large scale IT systems in close cooperation with the national data protection authorities;
- **Inspections**
We will improve our methodology for inspections and visits, in particular a more streamlined method for inspecting IT systems.

Policy and consultation

As part of the delivery of the EDPS Strategy for 2015-2019, five key areas have been identified for our policy and consultation work in 2015:

- **Big data and the digital single market**
We will present a vision for how the EU should ensure individuals are able to exercise user control, enjoy the benefits of big data and ensure organisations and businesses are transparent and accountable for the personal data processing for which they are responsible. We will elaborate the vibrant debate stimulated by our Preliminary Opinion on competition law, consumer protection, privacy and the digital economy by participation in events and discussion with regulators.
- **Finalising the reform of the data protection framework**
Before summer 2015, we will present a policy briefing for the institutions to inform and help find practical and flexible solutions during the forthcoming trilogue on the General Data Protection Regulation and the Directive on data protection in law enforcement cooperation. We will also turn our focus, in close cooperation with national supervisory authorities, to implementation of the new rules. In particular, we will help prepare for a seamless transition to the new European Data Protection Board, without prejudice to the co-legislators future decision on the organisation of the Board's secretariat. We will engage in the early stage policy discussion on the development of implementing or sector specific legislation, such as any proposal to reform Directive 2002/58/EC.
- **International agreements**
We will work proactively with EU institutions to ensure data protection principles are properly and consistently taken into consideration when negotiating international agreements on trade as well as law enforcement, such as TTIP, TISA and Safe Harbour and the scheduled automatic renewal of the TFTP agreement with the US. We will also offer our expertise and assistance where appropriate in the monitoring of existing agreements, such as the bilateral agreements on PNR.

- **Equipping policymakers in the home affairs sector**

In liaison with experts from the Commission, we aim to prepare guidelines on integrating data protection rules and principles in proposals and policies on internal security, border management and migration. The new European Agenda on Security needs to include more convergence between different data protection laws in this area and consistency in the supervision of large-scale IT systems. On specific measures, such as an EU PNR directive and the 'Smart Borders' package where discussions are ongoing, we have offered to work with the institutions to find ways to minimise intrusiveness into the rights to privacy and to data protection of the vast number of individuals potentially affected. Our advice will be predicated on recent case law especially the CJEU judgment on the Data Retention Directive in Digital Rights Ireland. We will also prepare a background paper developing the concepts of necessity and proportionality, especially in the light of recent case law, and how they should be applied to proposals which have an impact on data protection.

- **Agreeing working methods with the EU institutions and bodies**

As announced in our Policy Paper, we will seek to agree efficient ways of working with the institutions, where appropriate through memoranda of understanding, in discharging our policy and consultation role. We will seek feedback on the value of our advice. This will build on recent close cooperation with the Italian presidency on a draft directive on the automatic exchange of bank account information between tax authorities. We will continue to liaise closely with the Fundamental Rights Agency on issues of common concern.

Cooperation

Our ambition is for the EU to speak with a single voice on questions of privacy and data protection. Therefore the central motor of our strategy will be close cooperation with fellow data protection authorities.

- **Coordinated supervision**

We will continue to prioritise efficient and loyal engagement and support in the coordinated supervision of CIS, EURODAC, IMI, SIS II and VIS. Our aim is to move to a more consolidated and

effective governance model for systems under the former 'third pillar'.

- **Article 29 Working Party**

We will engage closely with the Working Party not only to ensure a smooth transition to the EDPB, but also in developing and contributing to policy opinions both in subgroup and in plenary meetings, as rapporteur where appropriate, and in the operational supervision of EU agencies and IT systems.

- **Non EU countries and international organisations**

We will promote a global alliance with data protection and privacy authorities to identify technical and regulatory responses to key challenges to data protection such as big data, the internet of things and mass surveillance. We will also be fully involved in discussions on data protection and privacy at international fora including the Council of Europe and the OECD.

IT Policy

- **Data protection going digital**

One of our key actions to achieve this strategic objective will be to improve our alliance with stakeholders, particularly the technical community, in order to create more interdisciplinary cooperation on data protection by design and by default.

- **Internet Privacy Engineering Network**

We will continue to focus on data protection and privacy from an engineering perspective. As IPEN includes technology experts from DPAs, industry, academia and civil society, distinguishing it from other networks, IPEN efforts are directed to issues of practical relevance. In 2015, the network will expand and continue to work on lines of action established in 2014.

- **Technology monitoring**

Our technology monitoring activities will become more visible and made accessible to other stakeholders to inform their work. In addition to informing our own activities, the cooperation with DPAs and with technology-oriented expert groups at EU-level, we will make our reports accessible to the public.

- **Guidance on technology and data protection**

In order to promote a data protection culture in the EU institutions supervised by the EDPS, the

preparation of guidelines for specific technical areas, such as mobile devices, web services and cloud computing, will be concluded in 2015, complemented by guidance on specific areas such as risk management.

- **IT security**

The importance of IT security management has increased over the years. We will continue to develop our expertise in IT security and its systematic application as a supervisory authority in our inspection and auditing activities and as a partner in our cooperation with the IT security community, with particular focus on the EU Institutions.

Other fields

Information and communication

2015 is a year of change at the EDPS. With a new mandate and strategy, there is an atmosphere of anticipation and potential of what can be achieved over the next five years. As a reflection of this, there are several major information and communication projects that will be undertaken. Among them are:

- **A new visual identity**

A significant project for 2015 will be the revision of our visual identity which will entail a new logo and graphic chart. The knock on effect of the change in our visual identity is that all EDPS communication materials will also need to be updated (such as promotional items, publications, website and so on). Therefore, this will be a long-term project as we will continue to use the materials we have and update them when we run out or when it is no longer feasible to continue doing so.

- **Updating the EDPS website**

We will also be making some major technical updates to our website and we will use the opportunity to refresh the look and feel of it.

- **Clear language**

We have continued to make huge strides towards our clear language goal over the last few years. Our overriding aim is to correct the excessive legal and technical image of data protection. This remains a priority and so in 2015, we will continue our use of straightforward language to make technical issues more accessible, with examples that the general public can identify with.

Resource management and professionalising the HR function

The new EDPS mandate and strategy will entail changes that will impact our HR work and put additional pressure on a shrinking budget following several years of austerity policies.

- Among those changes, the likely adoption of a new Data Protection Regulation, replacing Directive 95/46/EC, may directly impact the organisational structure of the EDPS, particularly if, as provided in the Commission's proposal, the EDPS is entrusted with the provision of the Secretariat of the new European Data Protection Board (EDPB). Consequently, the budget for 2015 already includes a new Title III called the EDPB and an EDPB Task Force will be established in the second half of the year.
- In 2015, we will develop two papers that look at ways of increasing the accountability and ethical dimension of our institution: a new code of conduct for the team of Supervisors and a whistleblowing policy, further to the recommendations by the European Ombudsman.

In our aim of leading by example, we will cooperate very closely with the EDPS DPO on a privacy impact assessment and the revision of data protection notifications further to the entry into force of the new Staff Regulations.

www.edps.europa.eu



Publications Office

ISBN 978-92-9242-062-8



EDPS

EUROPEAN DATA PROTECTION SUPERVISOR