

Strategy

2013-2014

Towards excellence
in data protection



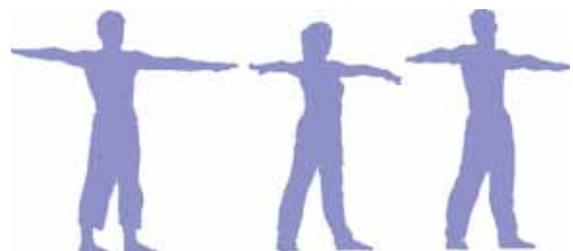
EUROPEAN DATA
PROTECTION SUPERVISOR



Strategy

2013–2014

Towards excellence
in data protection



**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**

(* Certain mobile telephone operators do not allow access
to 00 800 numbers or these calls may be billed.

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

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2012

ISBN 978-92-95076-72-3

doi:10.2804/51561

© European Union, 2012

Reproduction is authorised provided the source is acknowledged.

© Photos: European Parliament and iStockphoto/Edps

Printed in Belgium

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

CONTENTS

Foreword	5
Summary	7
The Report	
1. The mission of the EDPS	8
2. The developing role of the EDPS	9
3. The Strategic Review	11
4. The feedback from stakeholders	13
5. Core values and guiding principles	15
6. Action plan	17
7. Measuring performance	19



Peter Hustinx, Supervisor (centre), and Giovanni Buttarelli, Assistant Supervisor (right), with Christopher Docksey, Director (left), acting together as the Management Board

FOREWORD

This report sets out the Strategy for the Period 2013-2014 adopted by the European Data Protection Supervisor (EDPS). Although this is a two-year strategy, it aims to lay longer-term foundations.

We have developed the strategy in response to our increasing workload and the broader scope of activities that the EDPS will face in the coming years. Increasing exchanges of personal information and ever-evolving technologies mean that data protection's visibility and relevance are now greater than ever. At the same time, the Lisbon Treaty has considerably strengthened the rights to data protection and privacy in EU law. To improve the effectiveness of these rights, the European Commission proposed a new data protection legal framework in January 2012. This will have direct consequences for the EDPS.

In view of these challenges and the prevailing need to 'do more with less', we began a strategic review in 2011 to identify priorities and develop the strategy set out in this report.

The purpose of this strategy is to enable us to fulfil our commitments towards citizens and the EU institutions and bodies in a challenging and continuously evolving environment. With this report we also inform our stakeholders on how we will carry out our activities.

Our strategy has been developed through an extensive process of consultation with internal and external stakeholders. We are very grateful to all those who have given us their views, whether by responding to the online questionnaire, attending our internal conferences, or agreeing to participate in individual interviews and focus groups. Thank you: your many comments and creative ideas have helped us build the foundation for the strategy outlined in this report.



Peter HUSTINX
Supervisor



Giovanni BUTTARELLI
Assistant Supervisor



Christopher DOCKSEY
Director

Brussels, 22 January 2013

SUMMARY

The EDPS is the European Union's independent data protection authority. We monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals, and we advise the EU legislator on proposals for legislation and new policies. Data protection is crucial for society, as citizens become increasingly dependent on the use of information technology and as personal information is collected or generated on an ever-increasing scale.

This report explains the work and the strategy of the EDPS as we enter a new phase marked by new challenges, in particular an increase in our activities at a time of budget restraint. The report describes the consultation of internal and external stakeholders and their detailed comments on our work. This valuable input has enabled us to develop our guiding principles and to set a detailed action plan for achieving our strategic objectives. The report concludes with a list of performance indicators to measure success. These actions will maximise the impact of our work on data protection at EU level and increase efficiency by making the best use of resources.

In general, stakeholders have praised the EDPS as a knowledgeable and authoritative body, providing strong leadership and data protection expertise. However, they made several suggestions for action, including the need for the EDPS to engage more closely with stakeholders and better understand their policies and institutional constraints, to work harder to raise awareness of data protection and make it more accessible, to improve our

knowledge of IT issues, to be selective and focus on areas of high priority or high risk, and to support the Data Protection Officers (DPOs) and Data Protection Coordinators/Contact Points (DPCs) who are on the frontline of data protection in the EU institutions and bodies.

We have reassessed our priorities and reallocated our resources to increase our efficiency and effectiveness to take account of these suggestions. Using our expertise, authority and formal powers we aim to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions. Acting selectively and proportionately, we seek to ensure that data protection will be an integral part of policy-making and legislation, in all areas where the EU has competence. We will focus our attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy.

In particular, we have identified activities that emphasise the accountability of policy makers and data controllers and activities that build on the crucial role of DPOs. These activities are key parts of the proposed legislative reforms, and we hope they will show how levels of compliance can be raised in a period of budget restraint.

We will use this strategy over the period 2013–2014 and develop it further thereafter. This will better enable us to respond effectively to the challenge of achieving excellence in data protection at European level.

1. THE MISSION OF THE EDPS

The EDPS is the European guardian of data protection

The EDPS is the European Union's independent data protection authority. We monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals.



We advise EU institutions and bodies on all matters relating to the processing of personal information. We are consulted by the EU legislator on proposals for legislation and new policy development. We monitor new technology that may affect the protection of personal information. We intervene before the EU Court of Justice to provide expert advice on interpreting data protection law. We also cooperate with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information.

Data protection is crucial for society

The protection of personal data is vital for citizens of the information society. As we become increasingly dependent on the use of information technology (for example, using online payments, social networks and search engines) and as personal information is collected or generated on an ever-increasing scale, it is more important than ever that our individual liberties are adequately protected.

Data protection rules exist to protect individuals and facilitate the lawful processing of their personal information. The rules embody the right not to be on file or monitored in an abusive or uncontrolled manner. Their purpose is to enable individuals to exercise their rights and protect their legitimate interests.

The fundamental right to data protection and privacy can only be made a reality if data protection rules are effectively complied with in practice.

Ensuring the protection of the fundamental right to privacy

The EDPS is an independent authority with expertise in the field of EU data protection and the broader national and international arena. We aim to work strategically to promote a 'data protection culture' in EU institutions and bodies, thus contributing to improvements in good administration and effective risk management. We work to integrate respect for data protection principles in EU legislation and policies; and we seek to improve the quality of EU policies whenever effective data protection is a basic condition for their success. We are successful when we communicate the data protection message and enable and involve the stakeholders concerned. If necessary, we also use our powers of investigation and enforcement in order to ensure compliance.

Communicating data protection: a key condition for making it more effective

The EDPS aims to raise awareness of data protection and inform individuals on the existence and content of their rights. To gain public confidence, understanding and support, it is essential to have increased transparency of processing of personal information at EU level and more information on EU data protection. We, therefore, communicate in ways that are easy for the public to understand.

2. THE DEVELOPING ROLE OF THE EDPS

As a *regulator*, a supervisory and enforcement body, the EDPS is putting more pressure on the EU administration to raise its compliance with data protection rules. We do this by increasing our supervision and follow-up actions, with prior-checks, inquiries, visits and inspections. We have developed external tools to help data controllers to achieve compliance, providing better support to DPOs and DPCs such as training, guidelines and monitoring surveys. After the policy announcement in the EDPS Paper on Compliance and Enforcement of December 2010, we have increasingly applied our enforcement powers where necessary.

As an *advisor*, the EDPS is receiving more requests for informal and formal opinions both on administrative measures and legislative initiatives. Data protection is clearly expanding in all areas of EU policy as new instruments are created using IT tools to aid the exchange of information. We have also become an integral partner for the EU institutions, which regularly consult us when developing policy and legislation. Furthermore, we increasingly provide expert advice on interpreting data protection law in court cases, whether on our own initiative or at the Court's request.

Cooperation with other supervisory authorities is also increasing as a result of playing a more active role in the work of the fora of the EU's Data Protection Authorities (e.g. the Article 29 Working Party) as well as through the consolidation and expansion of the so-called *coordinated supervision* method. This is a model of supervision for large-scale European IT systems,



involving both the EDPS and national Data Protection Authorities (DPAs), where we act as the Secretariat.

In a hyper-connected world with evolving technologies and increasing exchanges of personal information, the protection of personal data requires *global, coordinated and cross-border approaches*. As a result, innovative initiatives to promote data protection have also been pursued by the EDPS in the International Conference of Data Protection and Privacy Commissioners, in the European Data Protection Conference, and in the context of the OECD, the Council of Europe and the Berlin group (international expert group on data protection and communications), as well as in a series of workshops on data protection as part of 'good governance' in international organisations.

As awareness of data protection issues within the EU administration has increased over the years, the *visibility* of the EDPS has also steadily increased. This has naturally given rise to greater interaction with EU and national institutions, citizens and media, with stakeholders referring more frequently to the EDPS on a broader range of issues.

Adapting to new challenges

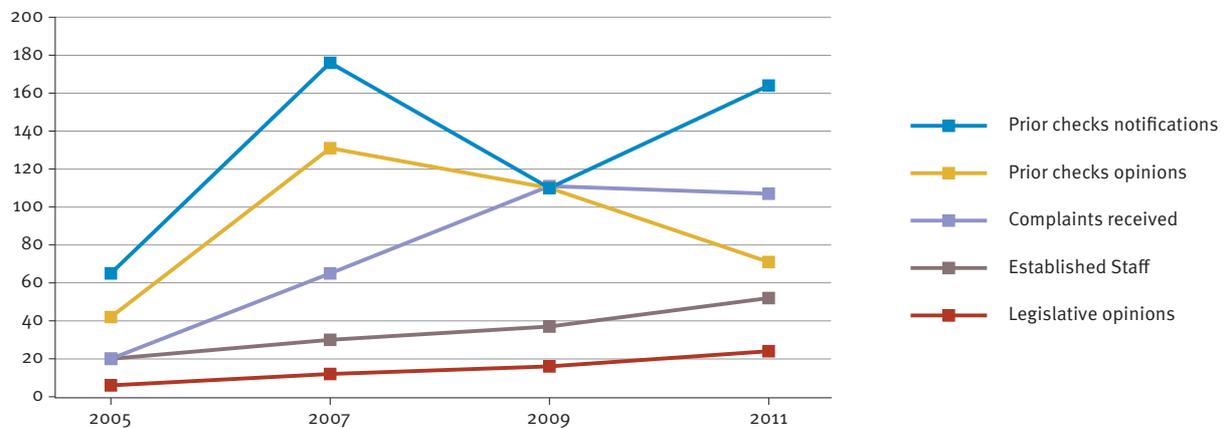
In addition to the increase in our activities, the EDPS faces several key developments:

- the accelerating use of the internet and new technologies
- the entry into force of the Lisbon Treaty and its emphasis on fundamental rights;
- the adoption and continuing implementation of a new policy programme for the area of freedom, security and justice (the Stockholm Programme) and the crucial importance of data protection in this area;

- the adoption, review and continuing implementation of the Commission strategy to generate growth and confidence in the internet (the Digital Agenda) and its impact on data protection in this area; and
- the ongoing review process of the EU data protection legal framework, including the sensitive issue of governance and its implications for cooperation between data protection authorities.

The Lisbon Treaty introduced a strong legal basis for comprehensive data protection in all areas of EU policy, which has put considerable pressure on the limited resources of the EDPS. The end of the traditional separation of EU policy ‘pillars’ (European Communities and Police and Judicial Co-operation in Criminal Matters) has led to a greater number of ‘law enforcement’ processing activities falling within the scope of EU law and thus becoming subject to the supervision of the EDPS.

The development of core activities and staffing levels



We set a deadline in Spring 2007 for so-called ‘ex-post’ prior checks¹, which resulted in the peak in prior checks seen in the above chart. Moreover, the EDPS now deals as far as possible with prior checks in common opinions on specific issues notified by a number of EU institutions and bodies. As a result, there has been a decrease in the number of prior check *opinions* in this chart but not an actual decrease in prior check *notifications* themselves.

The chart shows a marked increase over the years in all areas of EDPS activities, which require a considerable investment of resources, and that this has not been matched by staffing levels. The developments outlined above also indicate that the increase in our workload is likely to continue in most areas. To deal with this continuing increase efficiently and effectively, we will need to ‘do more with less’ within present staffing constraints.

¹ A backlog of processing operations started before the establishment of the EDPS, but requiring a prior check due to their nature, was processed by the EDPS and led to improvements of data protection in a number of cases.

3. THE STRATEGIC REVIEW

In July 2011, the Management Board began the strategic review process and appointed a Task Force to carry out the review.

We began by first defining the **strategic objectives** that will increase the effectiveness and impact of our core activities and thus maximise the impact of data protection at European level.

Our strategic objectives

1. 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
2. Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and integrates data protection in new legislation
3. 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

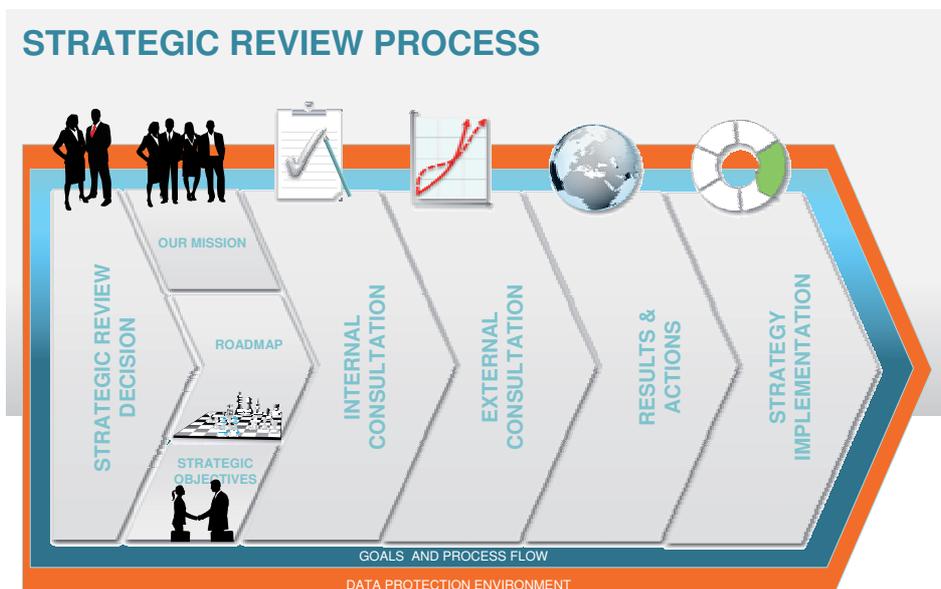
4. Develop an effective communication strategy
5. Improve the use of human, financial, technical and organisational resources.

Building on strengths

The review process builds on several substantive and organisational changes already made or in progress:

- In 2005, we published our policy on EU institutions consulting the EDPS, which is specified in public annual priorities (the policy inventory) and which guided our activities until the review.
- In 2008, we adopted our *Guidelines concerning the processing operations in the field of staff recruitment*, and our first training session for DPOs took place in 2011.

Flow-chart, below, summarises the different phases of the EDPS strategic review.



- In 2010, we adopted our new approach to compliance and enforcement.
- Also in 2010, we began reorganising the Secretariat by introducing a new institutional framework of units and sectors reporting to a Director. The process was completed in 2011 when we created a new sector on IT Policy.

Comments by stakeholders suggesting some of these changes underlined the need for improved communication on what the EDPS was already doing.

The consultation process

The review was conducted in two phases:

(a) internal consultation

The purpose of the internal consultation was to identify ways to improve the efficiency of the organisation so as to better respond to longer-term challenges and

opportunities. All staff were involved in defining the strategy.

Their ideas and proposals were discussed at the first EDPS internal conference, which took place on 25 October 2011. The outcome of the internal discussions laid the foundation for the external consultation.

(b) external consultation

The external stakeholders of the EDPS were consulted on how they perceive the activities of the institution, on what they think could be improved in the way we work with them and on how we could achieve this. The external consultation was launched in March 2012 with an online survey.

The Online Survey

The online survey was conducted on a sample of some 500 stakeholders divided into six main categories². The following table sets out the different groups surveyed, the numbers involved and the response rate (30% overall):

Stakeholder group	Number surveyed	Response rate
Data Protection Officer (DPO)/ Data Protection Coordinator/ Contact Point (DPC)	136	34%
EU Officials processing data (data controllers)	79	37%
EU Policy makers	180	17%
Other EU Institutions	17	71%
National Data Protection Authorities (DPAs)	71	24%
Civil society and other stakeholders	28	58%

Interviews and Focus Groups

We followed up the online survey with:

- 18 individual interviews, covering policy makers, data controllers, national DPAs, other EU institutions and civil society representatives, and
- 3 focus groups for DPOs, DPCs and data controllers.

We nominated the stakeholders for consultation via the online survey, by interview or in a focus group. However, the consultations were carried out by external consultants who operated the survey, who provided us with the aggregated feedback and analysis from stakeholders.

The results were discussed at a second EDPS internal conference in May 2012.

² journalists and newsletter subscribers were consulted more generally

4. THE FEEDBACK FROM STAKEHOLDERS

We took account of the stakeholders' feedback below when preparing our core values, guiding principles and the list of action points in parts 5 and 6.

Comments from all stakeholders

In general, stakeholders praised the EDPS as a knowledgeable and authoritative body, providing strong leadership and data protection expertise.

However, they made the following suggestions for action:

- the EDPS should engage more closely with stakeholders and not appear remote or bureaucratic
- Even so, the EDPS should maintain its independence and authority and achieve a constant balance between Parliament, Council and the Commission.
- the EDPS should work harder to raise awareness of data protection
- the EDPS should use plain and straightforward language to make a very technical subject more accessible
- the EDPS should demonstrate greater understanding of the policy, institutional contexts



and constraints of the other institutions and try to be more flexible and pragmatic (this point came from policy makers and data controllers)

- the EDPS needs to be selective and focus on areas of high priority or high risk.
- the DPOs and DPCs in the EU institutions and bodies are on the frontline of data protection at EU level and need to be supported in that role.

Several stakeholders said we needed to improve our knowledge of IT issues. We have already partly tackled this by creating the new IT Policy Sector in 2011. Its work is reflected in the Action Plan at part 6 below.

Comments by specific stakeholders

a) DPOs, DPCs and officials handling personal data (data controllers)

Whilst respondents felt that the EDPS is responsive, has authority and a high level of expertise, they felt we needed to:

- give more guidance, training and explanatory materials – this was requested both by DPOs/DPCs and by data controllers, who stressed the need for an educational rather than a punitive approach
- raise awareness among top management and data controllers – this would support the DPOs/DPCs and encourage data controllers to comply
- offer common tools and methods so that institutions and bodies can follow common positions on issues that apply to them all, such as HR and employment policies

- have a closer and more accessible dialogue with DPOs/DPCs and data controllers, who also highlighted the need for better understanding of their institutional context
- focus more strongly on high-risk processing activities, and
- apply more enforcement where there is unlawful processing of personal data – which would also support the work of DPOs/DPCs.

b) EU policy makers (in the Parliament, Council and Commission)

The policy makers said we were effective, knowledgeable and authoritative in informal consultations, but we needed to:

- gain greater influence by improving our participation in meetings and working groups
- increase awareness and understanding of data protection among EU policy makers, by providing more guidance and forums for interaction
- improve the coordination of responses we receive from data protection experts, and
- improve the feasibility of our advice by having a better understanding of institutional needs and context.

c) Stakeholders in other EU institutions (Fundamental Rights Agency, Internal Audit Service, Ombudsman, ENISA and the Court of Justice)

These respondents felt we were highly effective in communicating and giving clear advice, and they recognised we had a strong impact and the ability to influence policy. However, they said we needed to:

- improve style and tone
- develop more practical approaches – such as additional guidelines, seminars and presentations

- use clear and supportive language to convince senior staff in the institutions that data protection compliance would add value to their work, and
- support DPOs and use the DPO Network more.

d) National Data Protection Authorities (Article 29 Working Party *et al*)

These respondents recognised our leadership role and strong data protection expertise but said we should:

- offer more leadership at European level and act as a global data protection leader in the international arena
- improve the accessibility and effectiveness of our advice by making it more concise and practical
- offer a more effective bridge between the Working Party and Parliament, Council and the Commission, and
- maintain our impartiality between the EU institutions.

e) Civil society and other stakeholders (including business associations, privacy organisations, academia, law firms and data retention expert groups)

These respondents recognised our leadership role, data protection expertise, intellectual rigour and understanding of policy issues, but said we needed to:

- raise our profile and play a greater role in public debate and informing civil society
- improve our communication with the various stakeholders
- strengthen our ‘added value’ role – independence from other actors, influence at EU level, ability to coordinate data protection between the EU and other global actors.

5. CORE VALUES AND GUIDING PRINCIPLES

The following principles set out how we approach our tasks and how we work with our stakeholders.

Our core values

We are guided by the following core values in all our work:

Impartiality – *working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.*

Integrity – *upholding the highest standards of behaviour and doing what is right even if it is unpopular*

Transparency – *explaining what we are doing and why, in clear language that is accessible to all*

Pragmatism – *understanding our stakeholders' needs and seeking solutions that work in practice.*

General principles

1. We serve the public interest to ensure that EU institutions comply with data protection policy and practice. We contribute to wider policy as far as it affects European data protection.
2. Using our expertise, authority and formal powers we aim to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions.

3. We focus our attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy. We act selectively and proportionately.

Specific principles, by activity

The following guiding principles complement and do not replace the fundamental principles of data protection.

1. We use our expertise and authority to exercise our supervision and enforcement powers. We aim to ensure the protection of personal information and a fair balance with wider policy and political objectives.
2. In our supervision and enforcement work:
 - 2.1. we recognise that institutions – data controllers and DPOs/DPCs – carry first-line accountability
 - 2.2. we seek to help institutions carry out their responsibilities effectively, ensuring that the right support, training and guidance are in place
 - 2.3. we use our powers of supervision to reinforce responsibility
 - 2.4. we are willing to use our powers of enforcement where necessary.
3. In our policy and consultation work:
 - 3.1. we seek to engage constructively with policy makers at an early stage of policy development

- 3.2. we seek creative solutions that support policy goals and the principles of personal privacy, drawing on our knowledge of law and technology
- 3.3. we work to find practical solutions, particularly in complex policy areas, which may require difficult balances to be struck and difficult judgments to be made
- 3.4. we seek to ensure that data protection will be an integral part of policy-making and legislation, in all areas where the EU has competence
4. Working with other data protection authorities and supervisory bodies:
 - 4.1. we build on our expertise and experience in European data protection law and practice
 - 4.2. we seek to improve consistency in data protection law across the EU.
5. We seek to be an authoritative body by developing and building the expertise and confidence of our staff to engage effectively with our stakeholders.



EDPS Members and Staff, Internal Conference of 25 October 2011

6. ACTION PLAN



To meet our objectives, we have assessed and prioritised our activities to reflect the review's internal and external results.

We have identified the following priorities for each strategic objective set out in part 3 above:

Objective 1 – *Promote a 'data protection culture' within the EU institutions and bodies so that they are aware of their obligations and accountable for complying with data protection requirements.*

- Provide guidance and training for data controllers, DPOs and DPCs.
- Increase awareness-raising initiatives within EU institutions and bodies through workshops, meetings, seminars, training, and conferences.
- Raise awareness of data protection at all managerial levels and in various fora.
- Promote dialogue with data controllers, DPOs and DPCs.

- Increase the number of our visits and inspections as an element of our compliance and enforcement policy.
- Promote and provide guidance on the application of the principles of 'Privacy by Design and Privacy by Default'.

Objective 2 – *Ensure that the EU legislator (Commission, Parliament and Council) is aware of data protection requirements and integrates data protection in new legislation.*

- Extend timely and authoritative advice to the EU legislator on all matters to do with processing personal information during all stages of legislation and policy development.
- Increase our use of the policy initiatives inventory, being more selective in identifying those initiatives in which respect for data protection is essential.
- Issue guidelines with advice to the legislator and policy makers on horizontal issues.
- Improve contacts with the EU legislative institutions at all levels. This includes regular informal contacts to provide early policy input and to remain influential until the end of the legislative process.
- Assess the privacy risks of new technologies by collecting and analysing information as appropriate.

Objective 3 – *Improve the good cooperation with DPAs and the Article 29 Working Party to ensure greater consistency of data protection in the EU.*

- Contribute actively to the Article 29 Working Party by participating in its subgroups, drafting opinions and other texts, and looking for greater synergy with its activities.
- Cooperate with other DPAs on technology-related policy and enforcement issues and exchange experience and best practice with their technology experts.
- Further develop the methods of, and issue guidelines for, the coordinated supervision of the increasing number of large-scale IT systems.

Objective 4 - *Develop a creative and effective communication strategy*

- Update and develop the EDPS website.
- Develop new communication tools to make EDPS core activities more visible.

- Raise awareness of data protection through workshops, meetings and seminars
- Use straightforward language to make technical issues more accessible.

Objective 5 - *Improve the use of EDPS human, financial, technical and organisational resources*

- Further develop business planning and monitoring.
- Implement an effective training policy to develop professional skills.
- Better plan, perform and monitor the spending of financial resources.
- Develop a more strategic management of human resources.
- Strengthen administrative cooperation with other EU institutions.
- Develop and implement a total quality management system.
- Modernise case and knowledge management.
- Develop the internal IT strategy of the EDPS.

7. MEASURING PERFORMANCE

To assess progress towards our objectives we will regularly measure the performance of the activities listed above. We have identified the activities which have a key role for the achievement of our goals as the basis for the following Key Performance Indicators (KPIs).

These KPIs will enable us to report on the impact of our work and the efficiency of our use of resources. They will be regularly reviewed and adapted if needed, to improve our future performance. We will include the first set of results in our Annual Activity Report 2013.

KPIs	Description
KPI 1	number of inspections/visits carried out.
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).
KPI 3	level of satisfaction of DPOs/DPCs on training and guidance.
KPI 4	number of EDPS formal and informal opinions provided to the legislator.
KPI 5	rate of implementation of cases in our policy inventory which we have identified for action.
KPI 6	number of cases dealt with by the Article 29 Working Party for which the EDPS has provided a substantial written contribution.
KPI 7	number of cases in which guidance is provided on technological developments.
KPI 8	number of visits to the EDPS website.
KPI 9	rate of budget implementation.
KPI 10	rate of training implementation for EDPS staff.

The European Data Protection Supervisor

Strategy 2013–2014 — Towards excellence in data protection

Luxembourg: Publications Office of the European Union

2012 — 19 pp. — 21 x 29.7 cm

ISBN 978-92-95076-72-3

doi:10.2804/51561

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- via EU Bookshop (<http://bookshop.europa.eu>);
- at the European Union's representations or delegations. You can obtain their contact details on the Internet (<http://ec.europa.eu>) or by sending a fax to +352 2929-42758.

Priced publications:

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

Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and reports of cases before the Court of Justice of the European Union):

- via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).



EUROPEAN DATA
PROTECTION SUPERVISOR

*The European guardian
of data protection*

www.edps.europa.eu



@EU_EDPS



Publications Office

ISBN 978-92-95076-72-3



9 789295 076723