



EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Annual Activity Report

2014

1. Introduction	5
2. Operational achievements	6
3. Resource management	6
4. Management and internal control systems	7
4.1 Characteristics and nature of activities and risks	7
4.1.1 THE MISSION OF THE EDPS	7
4.1.2 THE DEVELOPING ROLE OF THE EDPS	8
4.2 Strategy 2013-2014	11
4.2.1 EDPS STRATEGIC OBJECTIVES	11
4.2.2 ACTION PLAN	12
4.2.3 MEASURING PERFORMANCE	14
4.2.4 CORE VALUES AND GUIDING PRINCIPLES	16
4.3 Inter-institutional cooperation	17
4.4 Events during the year that affected reputation	17
4.5 Internal control management system	18
4.6 Internal evaluation of the internal control system and indicators underpinning the statement of assurance	19
4.7 Results of independent audit during the year	20
4.7.1 COURT OF AUDITORS	20
4.7.2 INTERNAL AUDIT SERVICE (IAS)	20
4.7.3 FOLLOW-UP TO THE EUROPEAN PARLIAMENT'S DISCHARGE RESOLUTION	21
4.8 Follow-up to reservations from previous years	22
4.9 Conclusions on the effectiveness of internal control	22
5. Reservations and impact on the statement	23
5.1 Materiality criteria	23
5.1.1 OBJECTIVES OF MATERIALITY CRITERIA	23
5.1.2 QUALITATIVE CRITERIA	23
5.1.3 QUANTITATIVE CRITERIA	24
5.1.4 CRITERIA OF THE INTERNAL AUDIT SERVICE	24
5.2 Reservations	24
5.3 Conclusion	24
6. Statement of assurance from the authorising officer by delegation	25
7. ANNEXES	27
Annex 1 : Summary of annual activity report	29
Annex 2 : Budget 2014	30
Annex 3 : Risk Register	32



1. Introduction

The Financial Regulation (Article 66(9))¹ provides that each **authorising officer by delegation** (AOD) shall send an [annual activity report](#) to their institution, together with financial and management information. This report shall present the achievements of their unit in relation to the resources used. It shall also be a management report on performance in the context of their task as AOD. This requirement is the logical consequence of paragraph 2² of this same article, which gives the AOD responsibility for internal controls.

In the annual activity report of the AOD, this latter must include a statement of assurance (“Statement”) based on their own judgment and on the information available in which the AOD:

- states that the information contained in his/her report gives a true and fair view;
- declares that s/he has reasonable assurance that the resources allocated to the activities described in the report have been used for their intended purposes and in accordance with principles of sound financial management, and that the control procedures put in place give the necessary guarantees as to the legality and regularity of the underlying transactions;
- confirms that the AOD is not aware of any matter not reported which could harm the interests of the institution.

¹ Financial Regulation, Article 66(9): “The authorising officer by delegation shall report to his or her institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

(a) the information contained in the report presents a true and fair view;

(b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management;

(c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The activity report shall indicate the results of the operations by reference to the objectives set, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems, including an overall assessment of the costs and benefits of controls.

No later than 15 June each year, the Commission shall send to the European Parliament and the Council a summary of the annual activity reports for the preceding year. The annual activity report of each authorising officer by delegation shall also be made available to the European Parliament and the Council.”

² Financial Regulation, Article 66(2): “For the purposes of paragraph 1, the authorising officer by delegation shall, in accordance with Article 32 and the minimum standards adopted by each institution and having due regard to the risks associated with the management environment and the nature of the actions financed, put in place the organisational structure and the internal control systems suited to the performance of his or her duties. The establishment of such structure and systems shall be supported by a comprehensive risk analysis, which takes into account their cost effectiveness.”

2. Operational achievements

Each year, the EDPS publishes an 'Annual Report' giving an overview of the objectives and achievements of the institution's work. Information on operational achievements can be found in the annual report³.

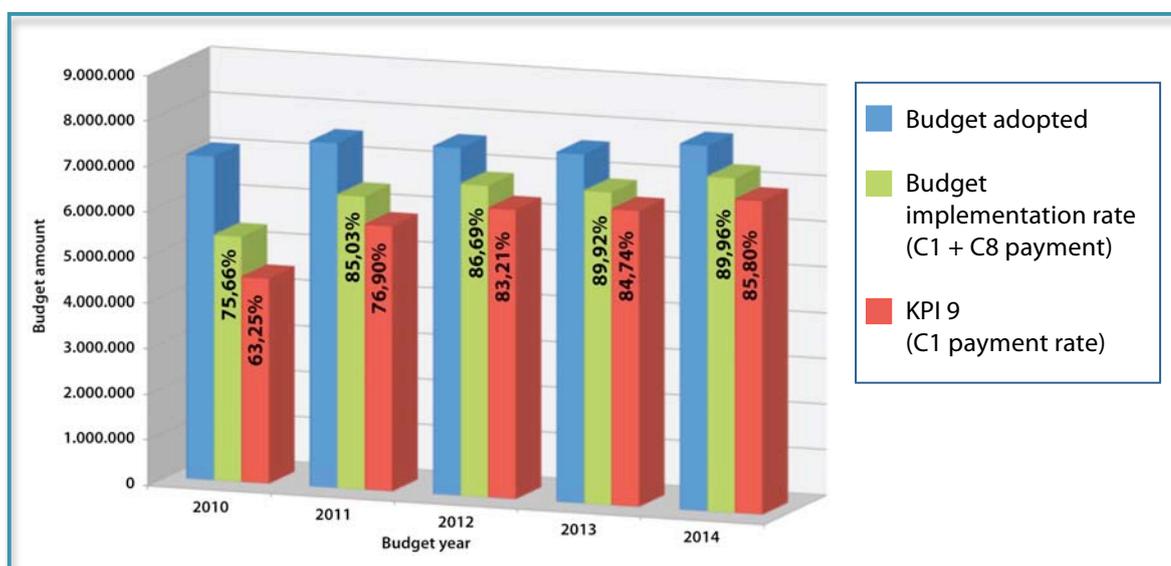
3. Resource management

The budget for 2014 adopted by the budgetary authority was EUR 8 012 953 (see Annex 2). This represented an increase of 4.59% compared to the 2013 budget.

As set in our KPI 9 (see table in page 12), the implementation rate in payment appropriations for 2014 was 85,8% as opposed to 84,7% for 2013.

The overall budget implementation rate for 2014 is expected to reach 92%.

EVOLUTION OF BUDGET IMPLEMENTATION 2010 - 2014



The EDPS applies the European Commission's internal regulations as regards budget implementation, insofar as these rules are applicable to the structure and size of the institution and provided that the EDPS has not adopted specific rules.

On the basis of the inter-institutional cooperation agreement, the Accounting Officer of the Commission has been appointed the Accounting Officer of the EDPS and the Internal Auditor of the Commission has been appointed the Auditor of the EDPS.

³ <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/lang/en/AR>.



4. Management and internal control systems

4.1. Characteristics and nature of activities and risks

4.1.1. THE MISSION OF THE EDPS

4.1.1.1. The EDPS is the European guardian of data protection

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

The EDPS also advises EU institutions and bodies on all matters relating to the processing of personal information. It is consulted by the EU legislator on proposals for legislation and new policy development. It monitors new technology that may affect the protection of personal information and intervenes before the EU Court of Justice to provide expert advice on interpreting data protection law. Finally, it cooperates with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal data.

4.1.1.2. Data protection is crucial for society

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

Data protection rules exist to protect individuals and facilitate the lawful processing of their personal information. They are closely related to the right that individuals have to private life, and must for instance ensure that individuals are not monitored in an abusive or uncontrolled manner. The 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.

4.1.1.3. Ensuring the protection of the fundamental right to privacy

The EDPS is an independent authority with high level expertise in the field of EU data protection and the broader national and international arena. His aim is to work strategically to promote ‘a data protection culture’ within EU institutions and bodies, thus contributing to improvements in good administration and effective risk management. It works to integrate respect for data protection principles in EU legislation and policies and seeks to improve the quality of EU policies whenever effective data protection is a basic condition for their success.

It is successful when it communicates the data protection message and involves all the stakeholders concerned. If necessary, it also uses his powers of investigation and enforcement to ensure there is compliance.

4.1.1.4. 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. This is why the EDPS communicates in ways that are easy for the public to understand.

4.1.2. THE DEVELOPING ROLE OF THE EDPS

As a **regulator** and a supervisory and enforcement body, the EDPS is putting more pressure on the EU administration to increase its accountability and full compliance with data protection rules. To do this the EDPS is intensifying his supervision and follow-up activities by carrying out prior checks, inquiries, visits and inspections. It has developed external tools to help controllers achieve compliance, providing better support to Data Protection Officers (DPOs) and Data Protection Coordinators (DPCs) such as training, guidelines and monitoring surveys. After the political announcement in the EDPS paper on compliance and enforcement of December 2010, he has increasingly applied his enforcement powers where necessary.

As an **advisor**, the EDPS is receiving more requests for formal and informal 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. It is now also an integral partner for the EU institutions, which regularly consult it when developing policy and legislation. Furthermore, it increasingly provides expert advice on interpreting data protection law in court cases, whether on his own initiative or at the request of the courts.

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 the national data protection authorities (DPAs), where the EDPS also acts as the Secretariat.

In a hyper-connected world with constantly changing 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.

The EDPS also focused on data protection and privacy from an engineering perspective. In 2014, the Internet Privacy Engineering Network (IPEN) was launched in collaboration with national data protection authorities, developers and researchers from industry, 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. A first workshop was organised in September 2014, establishing lines of action to be continued in 2015, together with the expansion of the network.

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.

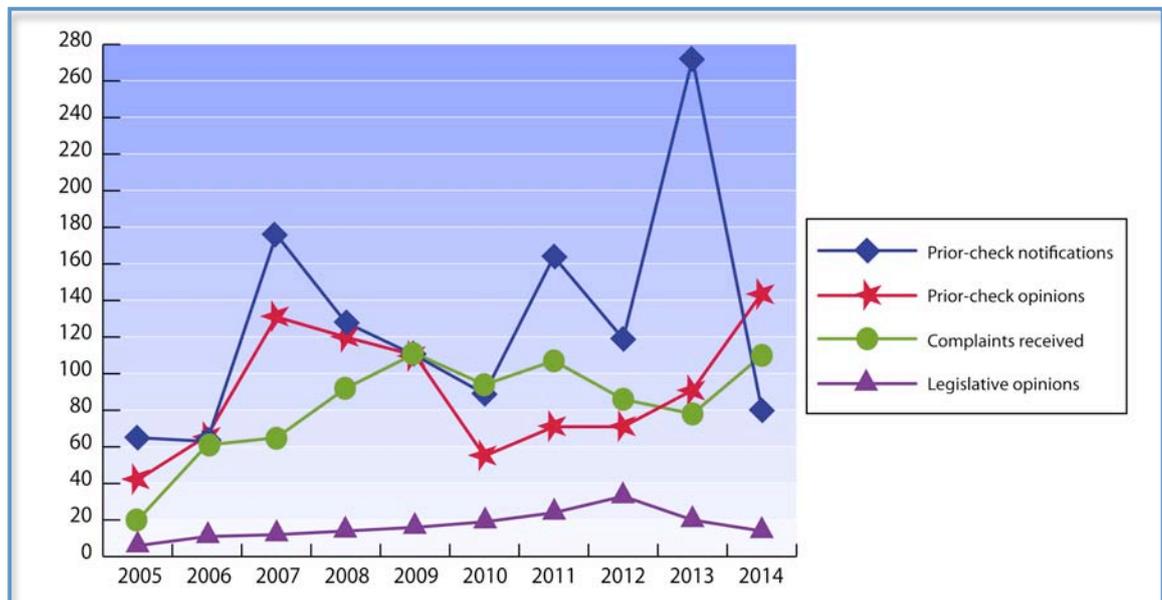
Adapting to new challenges

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

- the accelerating use of the Internet and new technologies, such as cloud computing and big data;
- the growing awareness of the risks of massive surveillance, and the need for appropriate responses, as accelerated by the recent revelations and allegations on intelligence activities;
- the growing role of fundamental rights in EU policies, as also underlined by the case law of the Court of Justice;
- the adoption and continuing implementation of multiannual programmes for the area of freedom, security and justice and the crucial importance of data protection in this area, in particular where the balancing of the needs of law enforcement with fundamental rights is at stake;
- the adoption, revision and continuing implementation of the Commission strategy to generate growth and confidence in the Internet (the Digital Single Market) and its impact on data protection, 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 cooperation in criminal matters) has led to a greater number of ‘law enforcement’ processing activities falling under the scope of EU law and thus becoming subject to the supervision of the EDPS.

The following graph shows a marked increase over the years in all areas of EDPS activities, requiring a considerable investment of resources, and yet staffing has not increased at a commensurate rate. The developments outlined above also indicate that the increased workload is likely to continue in most areas. To address this continual increase effectively and efficiently, the EDPS is requested ‘to do more with less’, within present staffing constraints.



The EDPS only has annual appropriations of a relatively small amount with which to perform his tasks. He has adopted the specific internal control procedures that he considers best adapted to his needs, in line with the size of the institution and its activities. The aim is to provide management with reasonable assurance that the institution’s objectives are being achieved and the risk management related to its activities is implemented. The EDPS has made progress in identifying the risks related to its increased activities, particularly through the adoption of a decision on risk management in July 2012. This facilitated a more structured approach towards risk management, as demonstrated by the adoption of a Risk register (see Annex 3) following the workshops held at the end of the year, as provided for in that decision. A revised decision on internal controls has been adopted in 2013.

The EDPS has no operational activities in the sense of activity-based budgeting, as in the Commission, but does have (limited) administrative expenditure. All financial and contractual commitments are submitted for the agreement of the authorising officer by delegation or sub-delegation and verified in advance by a member of his/her team. The internal financial verification system, the appointment of an Accounting Correspondent and the adoption of an ex post verification system have led to a considerable strengthening of the organisation’s internal controls.

4.2. Strategy 2013-2014

Strategy 2013-2014

In the **Strategy 2013-2014**, adopted in December 2012, the EDPS identified a number of strategic objectives to help increase the impact of its core activities on data protection at European level. To assess the progress towards these objectives, the EDPS identified the activities which play a key role in achieving those goals. The related key performance indicators (KPIs) helped the institution to monitor and adjust, if needed, the impact of its work and the efficiency of the use of resources.

This chapter reports on the performance of EDPS activities in 2014, in accordance with the objectives and action plans defined in the Strategy 2013-2014.

Overall, the results show a positive trend in the performance of the activities. The implementation of the strategy was on track and no corrective measures were needed.

4.2.1. EDPS STRATEGIC OBJECTIVES

The achievement of the **strategic objectives** aims at improving the effectiveness and impact of the core activities and thus maximise the impact of data protection at European level.

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 guarantee 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.**

4.2.2. ACTION PLAN

To meet those objectives, the EDPS has assessed and prioritised its activities to reflect the review's internal and external results. The institution identified the following priorities for each strategic objective set out in part V.2.1 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 controllers, DPOs and DPCs.
- Increase the number of his visits and inspections as an element of 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 his 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 data protection authorities, in particular the Article 29 Working Party, to guarantee greater consistency of data protection in the EU.

- Contribute actively to the Article 29 Working Party by participating in its subgroups, contributing also as rapporteur or coordinator to the drafting of 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 an 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.

4.2.3. MEASURING PERFORMANCE

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 EDPS will include the set of results in its Annual Report 2014, as done in 2013.

KPIs	Description	Results 2013	Target 2013
KPI 1	Number of inspections/visits carried out. <u>Measurement</u> : compared to target	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). <u>Measurement</u> : compared to target	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. <u>Measurement</u> : DPOs/DPCs satisfaction survey to be launched every time a training is organised or a guidance is issued	100% positive feedback	60% positive feedback
KPI 4	Number of EDPS formal and informal opinions provided to the legislator. <u>Measurement</u> : compared to previous year	Opinions: 15 Formal comments: 13 Informal comments: 33	<u>2013</u> <u>as benchmark</u> O: 20 - FC: 13 IC: 33
KPI 5	Rate of implementation of cases in our policy inventory which we have identified for action. <u>Measurement</u> : percentage of "Red" initiatives (where the deadline for comments has expired) implemented as planned in the Inventory 2013	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. <u>Measurement</u> : compared to previous year	27	<u>2013</u> <u>as benchmark</u> 13
KPI 7	Number of cases in which guidance is provided on technological developments. <u>Measurement</u> : compared to target	58	20
KPI 8	Number of visits to the EDPS website. <u>Measurement</u> : compared to previous year	194.637	<u>2013</u> <u>as benchmark</u> 293.029
KPI 9	Rate of budget implementation. <u>Measurement</u> : amount of payments processed during the year divided by the budget of the year	85,8%	85%
KPI 10	Rate of training implementation for EDPS staff. <u>Measurement</u> : number of actual training days divided by the number of estimated training days	87,4%	80%

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 almost 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 initiatives which we had identified were either deleted or delayed by the Commission (for instance, TAXUD negotiations with WTO and Russia).
3. Improve the good cooperation with Data Protection Authorities, 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.

4.2.4. CORE VALUES AND GUIDING PRINCIPLES

The EDPS took account of the stakeholders' feedback when preparing its core values, guiding principles and action plan in the Strategy 2013-2014. The following main principles set out how to approach tasks and how to work with stakeholders.

4.2.4.1. The core values

The EDPS is guided by the following core values in all its work:

- **Impartiality** – working within the legislative and policy framework given to it, 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 it is doing and why, in clear language that is accessible to all.
- **Pragmatism** – understanding its stakeholders' needs and seeking solutions that work in practice.

4.2.4.2. General principles

1. The EDPS serves the public interest to ensure that EU institutions comply with data protection policy and practice. He contributes to wider policy as far as it affects European data protection.
2. Using his expertise, authority and formal powers 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. He focuses his attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy. He acts selectively and proportionately.

4.3. Inter-institutional cooperation

The EDPS benefits from inter-institutional cooperation in many areas by virtue of Service Level Agreements with the Commission and a cooperation agreement with the Parliament. This administrative cooperation is vital for us as it increases efficiency and allows for economies of scale.

In 2014, we adopted a new security decision (EUCI) and continued our close cooperation with various Commission Directorates-General (Personnel and Administration, Budget, Internal Audit Service, Infrastructure and Logistics, Education and Culture), the Paymaster's Office (PMO); the European School of Administration (EUSA); and the Translation Centre for the Bodies of the European Union. This cooperation takes place by means of service level agreements, which are updated regularly.

Furthermore, this inter-institutional cooperation applies also to the Internal Audit Service of the European Commission, by means of an SLA and a Memorandum of Understanding (MoU) that was signed in full observance of their respective rights, obligations and independence.

4.4. Events during the year that affected reputation

There were no events during 2014 that might have had a negative impact on the institution's reputation.

4.5. Internal control management system

Internal control covers the globality of the policies and procedures put in place by the institution to ensure the economic, efficient and effective achievement of its objectives. In order to assess and improve the effectiveness of the internal control system, in 2013 the EDPS adopted 15 out of the 16 Internal Control Standards (ICS), laid down in the European Commission decision of 2007^{4 5}.

Since then an increasing number of implementing measures was put in place to provide effective internal control of the processes in place. By way of example, measures taken to implement the internal controls standards (ICS) include: a revised version of all job descriptions; internal rules of procedure adopted in December 2012 (based on Article 46(k) of Regulation (EC) No 45/2001); the presentation of unit activities to all staff; a guide to accessing documents and an annual risk assessment.

The four-level system of activities planning (strategic, annual, monthly and weekly) forms the basis on which the EDPS manages his workload.

According to Art. 13 of the EDPS Rules of Procedure, the EDPS shall establish each year an Annual Management Plan. That plan shall translate the long term strategy of the EDPS into general and specific objectives. Indeed he sets out the activities to be undertaken, by specific objective. In line with the Art. 13 the Annual Management Plan also includes the key performance indicators, defined in the Strategy 2013-2014, which were regularly measured to monitor progress achieved during the implementation phase.

Since the adoption of the decision on risk management in July 2012 –modern tools that help to identify the risks and possible plans of action- the EDPS has included risk management as an essential element of his global strategy. Risk management goes beyond assessing the risks, it also involves putting controls and measures in place that then need to be monitored (*see Annex 3*).

These controls put in place by the EDPS, along with the procedural channels, are intended to correct any financial or procedural error that might arise. They are an integral part of the management of the EDPS, as are any corrections to which they give rise. The AOD is thus aware of any corrections. Neither the nature nor the frequency of the identified risks has been significantly relevant.

⁴ Communication SEC(2007)1341.

⁵ Only ICS number 16 related to Internal Audit Capability is not applicable to the EDPS.

4.6. Internal evaluation of the internal control system and indicators underpinning the statement of assurance

The monitoring of the implementation of the ICS is the responsibility of the Internal Control Coordinator (ICC), who reports directly to the Director. Regular controls are carried out on the basis of a control matrix, which includes all the recommendations and actions to be undertaken in order to comply with the adopted ICS. The matrix is the object of regular reviews and updates. The ICC also meets with the EDPS units/sectors to ensure effective implementation.

Since July 2014 a report on the implementation of the ICS is established twice a year to assess their effectiveness. The report is submitted to the Management Board for adoption.

Furthermore, the ex-post facto verification and the accounting correspondent functions monitor, on a sample basis, the legality and regularity of the financial transactions as well as the quality of accountancy once a year.

This enables the institution to demonstrate that the overall internal control system is effective, not only that sufficient controls are in place but also that these controls take account of the risks involved and are effective.

At this stage, the AOD estimates that the level of management and control put in place is appropriate, and improving. Such improvements are not likely to have a 'material' impact within the meaning of paragraph 5.1. No reservations are necessary with regard to the improvements underway.

At the time of writing this annual activity report, no significant errors have occurred and no reservations are necessary as regards preventive controls.

No recommendations that are currently being implemented are therefore likely to have a material impact⁶.

⁶ The materiality criteria used for this judgment are given in Chapter 5.1 of this report.

4.7. Results of independent audit during the year

There are two kinds of independent audit applicable to the EDPS. The first is the work of the European Court of Auditors and the second is that of the institution's Internal Auditor.

4.7.1. COURT OF AUDITORS

The report of the Court of Auditors for 2014 has been received but is still confidential and provisional. As regard the legality and regularity of underlying transactions no payments were selected for 2014.

4.7.2. INTERNAL AUDIT SERVICE (IAS)

The Commission's Internal Audit Service is the internal auditor of the EDPS. To make sure that EDPS resources are effectively managed, the internal auditor conducts regular checks on EDPS internal control systems and on its financial transactions.

In June 2013 the IAS carried out a follow up audit, with the result of closing most of the follow up actions stemming from IAS recommendations made in previous audits on administrative processes.

In October 2013 the IAS performed a risk assessment covering EDPS' major processes, both operational (related to his mission) and administrative (supporting the operational tasks). The results of this exercise enabled the IAS to prepare the Strategic Internal Audit Plan for the period 2014-2016 with regard to the EDPS, which was submitted to the EDPS in January 2014 and followed up in October 2014.

4.7.3. FOLLOW-UP TO THE EUROPEAN PARLIAMENT'S DISCHARGE RESOLUTION

In the context of the European Parliament's budgetary discharge for the 2013 financial year, no questions were raised with regard to the EDPS. The follow up report prepared for our rapporteur summarises the actions taken by the EDPS in response to the observations accompanying the discharge decision for the previous year.

1. The EDPS Case Management System has been in production since October 2013 and is used by all teams as a central repository for EDPS case documents, in compliance with audit recommendations (see paragraph 5 below). The central repository increases efficiency by making it easier to guarantee security of information due to integrated access rights management and eases and accelerates the retrieval of relevant information by its improved file classification possibilities and search functionality. The system is regularly adapted to new requirements and its functionality is extended in order to optimize support to the EDPS operations.
2. The IT Policy sector was created in 2012 to develop and concentrate our expertise in information technology and data protection. This sector is made up of Technology and Security experts with experience both in practical IT issues and in policy and supervision matters, as well as certified competence in auditing and inspecting IT systems. The concentration of IT experts in one team has led to better access to the expertise by other teams, more comprehensive technological analysis and synergy effects through better coordination and cooperation. It has also enabled the EDPS to develop his competences in the technological domain, e.g. for the promotion of Privacy by Design and by Default principles and to provide more practical advice to data controllers on technological data protection measures.
3. All open recommendations made by the IAS in its previous reports have been closed, following the implementation of the requested actions by the EDPS. Also recommendation n°18 (Secure the data contained in the complaints), which was still open in the IAS Annual Internal Report 2013, has been closed following the implementation of the following actions :
 - a. The Case Management System has been operational since October 2013
 - b. Complaints are accessible to EDPS Staff on the basis of an access control list
 - c. The EDPS Security Policy was adopted on 18 February 2014.
4. The implementation of the EDPS Strategy 2013-2014 was monitored twice a year through a set of ten KPIs assessed against targets. The results for 2013 have been published in the EDPS Annual Report 2013 as well as in the AAR 2013. The same will be done for the results of 2014. A revision of the current KPIs will be undertaken in the new strategic review to be launched in 2015.

5. EDPS and IAS have concluded an SLA in 2012 in order to maintain the audit function beyond the end of the administrative cooperation agreement with the Commission which happened at the end of 2013. This gives the mandate to the IAS to carry out its audit engagement at the EDPS.
6. As recommended by the Committee on Budgetary Control in the European Parliament, the EDPS Annual Activity Report includes every year a chapter on the actions taken in response to the discharge resolutions as well as an exhaustive table of all the human resources at the EDPS' disposal.
7. As to the Statement of Assurance concerning the financial year 2013 (DAS 2013), no observations resulted from the audit work carried out by the Court of Auditors with respect to the reliability of the annual accounts and the annual activity report of the EDPS.

4.8. Follow-up to reservations from previous years

The EDPS issued no particular reservations at the end of previous years.

4.9. Conclusions on the effectiveness of internal control

In light of the information above, the authorising officer by delegation considers that the internal control system is operating appropriately; bearing in mind the level of expenditure and budget handled by the institution, and thus gives the necessary assurance to his annual statement.



5. Reservations and impact on the statement

5.1. Materiality criteria

In order to establish the Statement of Assurance the AOD applies the materiality criteria adopted by the Court of Auditors.

5.1.1. OBJECTIVES OF MATERIALITY CRITERIA

The materiality threshold gives the AOD a basis on which to establish the significant weaknesses that require a formal⁷ reservation to his statement. The assessment of a weakness falls to the qualitative and quantitative judgment of the authorising officer by delegation, who remains responsible for the statement of assurance, including the reservations made.

The purpose of this chapter is to define the qualitative and quantitative criteria for determining the level of materiality.

5.1.2. QUALITATIVE CRITERIA

The following parameters were used to establish significant weaknesses:

- significant/repeated errors without mitigation
- weakness in the internal control system
- insufficient supporting documents
- material problems identified by the Court of Auditors or the Internal Audit Service
- problem of reputation.

⁷ The Commission (COM(2003)28 of 21 January 2003) considers that only 'material' reservations can be used to qualify the annual statement.

5.1.3. QUANTITATIVE CRITERIA

Once a significant weakness has been identified, quantitative criteria must be applied to determine the level of materiality. This level will be used to determine whether the weakness 'merits' being reported.

- margin of error
- maximum amount of risk

The Court of Auditors uses a 2% materiality threshold. Should the residual risk of an error be higher, the institution must explain the reasons for this.

The EDPS has decided on 2% of annual appropriations as the materiality threshold in this regard, namely: EUR 160 259,06.

5.1.4. CRITERIA OF THE INTERNAL AUDIT SERVICE

A 'table of significance' is added to the internal auditors' report.

In this table, a distinction is made between recommendations and observations on the one hand, and levels of importance on the other: critical, very important, important and desirable.

According to the internal auditors, only 'critical' level observations *may* result in a reservation in the statement given in the annual activity report. For the EDPS, there are no observations at this level.

5.2. Reservations

No reservations.

5.3. Conclusion

Based on the above, the Director of the EDPS Secretariat has issued the annual statement with no reservations.



6. Statement of assurance from the authorising officer by delegation

I, the undersigned, Christopher DOCKSEY,

Director of the EDPS Secretariat,

as Authorising Officer by Delegation

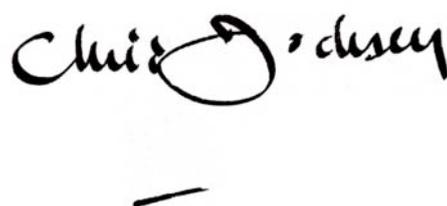
hereby declare that the information contained in this report is true and faithful.

I state that I have had reasonable assurance that the resources allocated to the activities described in this report have been used for the purposes anticipated and in accordance with the principle of sound financial management, and that the control procedures established provide the necessary guarantees as to the legality and regularity of the underlying operations.

This reasonable assurance is based on my own judgment and on the information available to me, such as the results of the self-evaluation and the report of the Internal Audit Service.

I confirm that I am not aware of any matter not reported that might be harmful to the institution's interests.

Signed at Brussels on 21 May 2015.



—



EUROPEAN DATA PROTECTION SUPERVISOR

Annexes



Annex 1 :

Summary of annual activity report

The Financial Regulation (Article 66(9))⁸ provides that the ***institution*** shall submit to the budgetary authority (European Parliament and Council), no later than 15 June each year, a summary of the annual activity report for the previous year.

Alongside this, Article 48 of Regulation (EC) No 45/2001 provides that the EDPS shall submit an annual activity report to the European Parliament, the Council and the Commission.

The proposal is thus to summarise the authorising officer by delegation's annual activity report and include this summary in the activity report that is provided for in Article 48 of Regulation (EC) No 45/2001:

Overall, the European Data Protection Supervisor considers that the internal control systems in place provide reasonable assurance as to the legality and regularity of the operations for which the institution is responsible.

The European Data Protection Supervisor will ensure that his authorising officer by delegation continues his efforts to guarantee that the reasonable assurance given in the statement attached to his activities report is effectively backed up by appropriate internal control systems.

⁸ Financial Regulation, Article 66(9): "The authorising officer by delegation shall report to his or her institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

- (a) the information contained in the report presents a true and fair view;
- (b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management;
- (c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The activity report shall indicate the results of the operations by reference to the objectives set, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems, including an overall assessment of the costs and benefits of controls.

No later than 15 June each year, the Commission shall send to the European Parliament and the Council a summary of the annual activity reports for the preceding year. The annual activity report of each authorising officer by delegation shall also be made available to the European Parliament and the Council."

Annex 2 :

Budget 2014

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION	2013	2014	2014 vs 2013	2014 vs 2013 (%)
CHAPTER 10 MEMBERS OF THE INSTITUTION				
Article 100 Remuneration, allowances and other entitlements of Members				
Item 1000 Remuneration and allowances	644.322,00	617.459,00	-26.863,00	-4,17%
Item 1001 Entitlements on entering and leaving the service		130.000,00	130.000,00	
Item 1002 Temporary allowances	0,00	50.000,00	50.000,00	
Item 1003 Pensions	32.000,00	40.000,00	8.000,00	25,00%
Item 1004 Provisional appropriation	0,00	8.700,00	8.700,00	
TOTAL Article 100	676.322,00	846.159,00	169.837,00	25,11%
Article 101 Other expenditure in connection with Members				
Item 1010 Further training	4.732,00	15.000,00	10.268,00	216,99%
Item 1011 Mission expenses, travel expenses and other ancillary expenditure	59.394,00	59.394,00	0,00	0,00%
TOTAL Article 101	64.126,00	74.394,00	10.268,00	16,01%
TOTAL CHAPTER 10	740.448,00	920.553,00	180.105,00	24,32%
CHAPTER 11 STAFF OF THE INSTITUTION				
Article 110 Remuneration, allowances and other entitlements of officials and temporary staff				
Item 1100 Remuneration and allowances	3.872.366,00	3.994.562,00	122.196,00	3,16%
Item 1101 Entitlements on entering, leaving the service and on transfer	70.564,00	50.000,00	-20.564,00	-29,14%
TOTAL Article 110	3.942.930,00	4.044.562,00	101.632,00	2,58%
Article 111 Other staff				
Item 1110 Contract staff	158.917,00	197.389,00	38.472,00	24,21%
Item 1111 Cost of traineeships and staff exchanges	179.428,00	179.428,00	0,00	0,00%
Item 1112 Services and work to be contracted out	51.202,00	51.202,00	0,00	0,00%
TOTAL Article 111	389.547,00	428.019,00	38.472,00	9,88%
Article 112 Other expenditure in connection with staff				
Item 1120 Mission expenses, travel expenses and other ancillary expenditure	112.686,00	112.686,00	0,00	0,00%
Item 1121 Recruitment costs	6.789,00	6.789,00	0,00	0,00%
Item 1122 Further training	84.874,00	78.500,00	-6.374,00	-7,51%
Item 1123 Social service				
Item 1124 Medical service	14.844,00	14.844,00	0,00	0,00%
Item 1125 Union nursery centre and other day nurseries and after-school centres	80.000,00	80.000,00	0,00	0,00%
Item 1126 Relations between staff and other welfare expenditure	3.865,00	6.000,00	2.135,00	55,24%
TOTAL Article 112	303.058,00	298.819,00	-4.239,00	-1,40%
TOTAL CHAPTER 11	4.635.535,00	4.771.400,00	135.865,00	2,93%
TOTAL TITLE 1	5.375.983,00	5.691.953,00	315.970,00	5,88%

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2013	2014	2014 vs 2013	2014 vs 2013 (%)
CHAPTER 20 BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION					
Article 200	Rents, charges and buildings expenditure	798.516,00	885.000,00	86.484,00	10,83%
TOTAL Article 200		798.516,00	885.000,00	86.484,00	10,83%
Article 201	Expenditure in connection with the operation and activities of the institution				
	Item 2010 Equipment	229.086,00	350.000,00	120.914,00	52,78%
	Item 2011 Supplies	19.524,00	15.000,00	-4.524,00	-23,17%
	Item 2012 Other operating expenditure	98.368,00	105.000,00	6.632,00	6,74%
	Item 2013 Translation and interpretation costs	875.000,00	775.000,00	-100.000,00	-11,43%
	Item 2014 Expenditure on publishing and information	150.000,00	112.000,00	-38.000,00	-25,33%
	Item 2015 Expenditure in connection with the activities of the institution	114.932,00	79.000,00	-35.932,00	-31,26%
TOTAL Article 201		1.486.910,00	1.436.000,00	-50.910,00	-3,42%
TOTAL CHAPTER 20		2.285.426,00	2.321.000,00	35.574,00	1,56%
TOTAL TITLE 2		2.285.426,00	2.321.000,00	35.574,00	1,56%
TOTAL BUDGET		7.661.409,00	8.012.953,00	351.544,00	4,59%

Annex 3: Risk Register

The EDPS has implemented a risk management exercise in 2014 with a risk analysis performed by all units and sectors of the Institution. Workshops took place in order to establish the possible risks and the related mitigating measures.

The results of this exercise are summarised in the table below:

Risk title & description (cause and effect)	Policy area & Activity/objective affected	Gross risk score			Controls	Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action			
		Likelihood	Impact	Overall score (L x I)			Likelihood	Impact	Overall score (L x I)		Frequency	Monitor		Action	Owner	Deadline	
Reputational risk due to malicious attacks in the press, attacks by complainants, e.g. the complaint to the LIBE committee, allegations for political purposes of bad internal administration and budgetary practices made to Court of Auditors and before the EP Budget Committee, e.g. "EDPS travel agency"	All EDPS activities	4	5	20	Accountability of staff on their daily work (handle contracts, respect deadlines, follow-up, etc.) Processes and procedures in place (ICS 8) Internal Control System in place (AAR, ICC)		3	5	15	Reduce	avoid - transfer - reduce - accept	Frequency	Monitor	Good = 1 Ok but so/so = 2 Pretty dreadful = 3	Code of conduct for Supervisors Establish new procedures (RM, monitoring of activities, whistleblowing, etc.) Strengthen accountability of staff on their daily work (handle contracts, respect deadlines, follow-up, etc.)		12/2015
Missing legal deadlines for access to document requests could have financial and reputational consequences for the EDPS	Directorate Objective affected: Implementation of strategies and policies of the EDPS in the context of the application of Regulation (EC) N° 1049/2001	4	5	20	Teams normally inform the Director as soon as the request arrives, so that he can reply		3	5	15	Reduce	Reduce	Frequency	Monitor		Establish procedure for timely processing of requests Raise awareness at weekly's and monthly's	Directorate + P&C	03/2015
Inadequate management of the Director's agenda could lead to miss important appointments and have a reputational impact on the Institution	Directorate Objective affected: Representation of the EDPS in relations with other institutions and bodies	4	4	16	Daily check of Director's calendar		3	3	9	Reduce	Reduce	Frequency	Monitor		Alerts in secretary's calendar Strengthen follow-up of Director's calendar	MCH	12/2015

Risk title & description (cause and effect)	Policy area & Activity/objective affected	Gross risk score			Controls	Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action		
		Overall score (L x I)	Impact	Likelihood			Overall score (L x I)	Impact	Likelihood		Risk	Monitor		Frequency	Action	Owner
Inconsistent position of the EDPS* (i.e. in providing advice, speaking at conferences, etc.)	Supervision & Policy Action point affected: Perform supervisory and consultation activities with excellence	5	4	20	HoA/HoU to ensure consistency Internal communication to be continued (weekly meetings) Ensure consistent application of case manuals Nomination of HoAs Communication with other teams (SILOS)		3	4	12	Reduce			Centralise information on case law Adoption of annotated version of Regulation		12/2015	
Not meeting the targets set in the AMP	Supervision Action point affected: Increase enforcement	4	4	16	Selective approach to the AMP increasing staff		4	3	12	Reduce			Consider delegation of signature E-signature	EDPS	01/2015	
Losing expertise	Policy Objective affected : Effective and efficient implementation of EDPS activities	4	4	16	Welcome package Case manuals Adequate training Back-ups		4	3	12	Reduce			Retention policy Fully detailed handover note (establish template) CMS: a) Repository for big issues (incl briefings and speeches) b) up-to-date state of play/ completed folders	All units + HRBA LP Case officer	03/2015 06/2015 12/2015	
Ineffective cooperation with EU institutions	Policy Action point 2 Cooperation with WP29, the Institutions and other Stakeholders 2.b Cooperation with Commission, Council & EP	4	5	20	Encourage personal contacts + initiatives via new internal inventory Organize workshops, guidelines Raising awareness Policy Paper The Secretary General's letter to EC of 8/12/06 regarding consultation of the EDPS		2	4	8	Reduce			Organise workshops on policy cooperation (Policy Paper) Regular meetings with DG Just and Home MoU	IC ABu ABo ABu CDC CD	12/2015 12/2015	

* The risk of inconsistency was highlighted by S&E and P&C units. Both units scored the reputational impact on EDPS very high, whereas P&C considers the mitigating measure in place sufficient to reduce the risk to an acceptable level.

Risk title & description (cause and effect)	Policy area & Activity/objective affected	Gross risk score			Controls	Person responsible & supervisor	Net (residual) risk score			Risk response	Monitoring		Control effectiveness	Further action		
		Overall score (L x I)	Impact	Likelihood			Overall score (L x I)	Impact	Likelihood		avoid - transfer - reduce - accept	Monitor		Frequency	Action	Owner
Service providers do not provide services as agreed or do not respond on time (or not at all) to demands.	<i>ITP</i> Objective affected: Improve the use of the EDPS human, financial, technical and organisational resources	5	3	15	Establish clear agreements with service providers and proper monitoring at the EDPS Establish escalation path for problems		3	3	9	Reduce			Service provider (Fabasoft) for IT security services Establish monitoring procedure for CMS operations		12/2015	
Compromise of service providers infrastructures	<i>ITP</i> Objective affected: Improve the use of the EDPS human, financial, technical and organisational resources	5	5	25	Implement dialogues with service providers on risks and security measures +Establish escalation path for problems Raise staff awareness (i.e. Monthly on IT security) +Apply effective technical security measures		5	3	15	Reduce			Encrypted email project Information security policy	FS AG	12/2015 12/2015	
Compromise of private equipment used by EDPS staff for professional purposes	<i>ITP</i> Objective affected: Improve the use of the EDPS human, financial, technical and organisational resources	5	5	25	Adopt relevant security policies + raise staff awareness + implement effective technical security measures + Mobile devise guidelines		4	3	12	Reduce			IP range verification	AG	12/2015	
No timely updating of the website	<i>Communication</i> Objective/activity affected: Publishing on the website Visibility and publicity of EDPS activities	4	5	20	Re-prioritise activities so that publication requests on the website are at the top Raising awareness of the teams that timely publishing on website is essential.		2	4	8	Reduce			Continue to assign more resources to the task	OR	12/2015	
Lack of Human resources in the Comm ^o team	<i>Communication</i> Objective/activity affected: All I&C activities	3	5	15	More resources		2	5	10	Reduce			Recruitment procedure for Contract Agent to be launched	OR	03/2015	

Risk title & description (cause and effect)	Policy area & Activity/objective affected	Gross risk score			Person responsible & supervisor	Net (residual) risk score	Risk response	Monitoring		Control effectiveness	Further action		
		Likelihood	Impact	Overall score (L x I)				Frequency	Monitor		Action	Owner	Deadline
Failure to capture external request in system	<i>RMG</i> Objective affected: to implement best practice in records management incorporating principles of data protection and transparency (access to documents)	Likelihood	5	5	25	Overall score (L x I)	Reduce			Good = 1 Ok but so/so = 2 Pretty dreadful = 3	Train third colleague for further back-up. Consolidate procedure for handling with mailbox	LP	04/2015
		Impact	5	5	5								
		Overall score (L x I)	5	5	25								
Late alert to RMG with regard to urgent deadlines	<i>RMG</i> Objective affected: meet the deadline with no errors in the output	Likelihood	3	5	15	Overall score (L x I)	Reduce				Update procedure for RMG dealing with short deadline and last minute requests information	LP	06/2015
		Impact	5	5	5								
		Overall score (L x I)	3	5	15								
Ineffective personal data protection notwithstanding high level of formal compliance	<i>DPO</i> Objective affected: Ensure compliance of the institution with the Reg. 45/2001	Likelihood	4	5	20	Overall score (L x I)	Reduce				EDPS accountability program / privacy policy Establish a review plan for notifications ex. Art 25	DPO	12/2015
		Impact	5	5	5								
		Overall score (L x I)	4	5	20								
Personal data security breaches	<i>DPO</i> Objective affected: Ensure compliance of the institution with the Reg. 45/2001	Likelihood	4	5	20	Overall score (L x I)	Reduce				Personal data breach procedure	ITP/ LISO/ DPO	10/2015
		Impact	5	5	5								
		Overall score (L x I)	4	5	20								



EUROPEAN DATA PROTECTION SUPERVISOR