2017-045

From: Fernando Silva, Data Protection Officer

To: eu-LISA Management Board

Subject DPO Annual Work Report - 2016

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
Rävala pst 4 • 10143 Tallinn • Estonia

Protection level **PUBLIC**

DPO Annual Work Report - 2016

Data Protection Officer

Table of Contents

1. Introduction 4
2. DPO activities and actions 4
2.1. Monitoring and compliance 4
2.1.1. Data Protection Awareness 4
2.1.2. Notification and register process 5
2.1.3. Annual Survey 6
2.1.4. Data Breaches 6
2.1.5. Other procedures and policies 6
2.1.6. Opinion and Guidance 7
2.2. Supervision by the EDPS and others 8
2.2.1. Inspections by EDPS to core systems 8
2.2.2. Supervision Coordination Groups – Eurodac, VIS and SIS II 8
2.2.3. DPO's Network meeting 8
2.2.4. Collaboration with other entities 9
2.2.5. JHAA DPOs Meeting 9
2.3. SISII, VIS and Eurodac – Opinion and guidance 10
2.4. Publications and policies 11
2.5. Complaint procedure 12
3. Conclusions 12
Glossary on definitions 13

Document Control Information

Settings	Value
Document Title:	Report on the annual activities of the DPO
Document Author:	POCAS DA SILVA, Fernando (DPO)
Revision Status:	Final
Issue Date:	27/02/2017

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*06/02/2017*	DPO	Initial version of the document created
[2]	*27/02/2017*	DPO	Revised version of the document

1. Introduction

On 23 December 2013 the Management Board of eu-LISA adopted the Decision 93/2013 on the Implementing Rules relating to Regulation (EC) No 45/2001 (hereinafter "the Regulation") of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "The Implementing Rules").
The Implementing Rules sets the data protection principles and rules applicable to eu-LISA as well as clarifies role and tasks of the Data Protection Officer (DPO) concerning the monitoring and supervising of those rules and principles. It is required also that the DPO shall monitor and ensure that the provisions laid down in the Regulation are applied by eu-LISA. The European Data Protection Supervisor (EDPS) shall in cooperation with the DPO, supervise the compliance of the Agency with the Regulation.
Under the Implementing Rules, the DPO is required to prepare and transmit to the Management Board an annual report on the status of compliance of eu-LISA with the Regulation, Article 6.1.e) of the Implementing Rules. This report illustrates the work performed by the DPO during the year 2016.

2. DPO activities and actions

The following sections will explain by topic the activities and the actions carried out by the DPO during the year 2016 in relation to monitoring and ensuring compliance at eu-LISA with Regulation 45/2001 and will assess the status of the compliance of the Agency.

2.1. Monitoring and compliance

The following sections present the work done on ensuring proper compliance with the Regulation and monitoring.

2.1.1. Data Protection Awareness

One of the key missions of the DPO is to raise data protection awareness among eu-LISA staff. During the year 2016, the DPO held the following awareness sessions:

- 6 general data protection awareness sessions, including Tallinn, Strasbourg and Brussels;
- 1 awareness session training dedicated to the processing operations carried out by the HRT

Unit;

- 4 Sessions dedicated to personal Data Breaches;
- 1 session dedicated to the outcomes of the EDPS SISII Inspection;

The privacy and processing of personal data consciousness is something that still lacks at staff level. Despite the DPO organized the awareness sessions in advance and with due notice both for eu-LISA Tallinn, Brussels Office and eu-LISA Strasbourg staff, this year attendance was lower than the previous ones, exception for the Brussels office were all staff attended.
The sessions were mandatory also for the contractors, the "*intra-muros*", in order to address the gap of requirements related with knowledge of personal data compliance as required by the eu-LISA Establishing Regulation.

The use of external contractors, the so-called "*intra-muros*" creates hindrances as the DPO notices in some cases a total absence on Data Protection principles that is linked to some lack of commitment to participate on the awareness session as they are for the staff.

As planned last year in order to make sure that the eu-LISA staff is instructed as soon as they start their functions in the Agency, the DPO in collaboration with the HRT Training Officer deployed a learning module with some interactive material as an induction phase for newcomers to know what data protection at eu-LISA is.

2.1.2. Notification and register process

The notification of processing operations on personal data is a legal requirement for the eu-LISA Controllers under the Implementing Rules and under the Regulation.
The number of notifications is growing with a boost coming from the end of last year. The DPO notes still a very high resistance on notifying processing operations on personal data. The reasons can be several, the workload that the staff in the Agency is subject, the lack of commitment towards the legal obligation, whether by the lack of interest or even information on the obligation to notify despite the DP awareness sessions.
In some cases even the position and comments of high managers towards the requests coming from the DPO, giving the opinion that data protection requirements are not reasonable at all, creating difficulties to the work of the DPO by undermining the role and importance of data protection rules.

The register of the processing operations is available, both forms and inventory of the processing operations notified to the DPO can be located under the common shared folder at Tallinn, in eu-LISA folder "19 Data Protection" and on the Common folder in Tallinn NAS on Data Protection.

At the end of 2016, 66 processing operations with personal data were notified to the DPO, 29

presented during the year. In total 5 required prior checking to the EDPS, but the DPO is preparing further requests.

2.1.3. Annual Survey

Another process launched by the DPO, with the intention to raise the personal data protection awareness, was the exercise of an annual survey carried out on HRT Unit, during the month of October 2014. The DPO finalised the survey report in May 2015. Due to the numerous changes in the HRT Unit some of the recommendations were no longer valid for the Unit. In middle 2016 the DPO presented the Report to the Executive Director.

The DPO intended to perform a survey to the GCU Unit, but the constant unavailability of the Head of Unit to perform the kick-off meeting, due to unforeseen events and heavy agenda, since September to the end-of-year, it was not possible to start the activity during 2016. The DPO reported the situation to the Executive Director and it was agreed to re-start the activity in 2017.

2.1.4. Data Breaches

During the reference period for this report, the DPO investigated five data breaches, two related with the large-scale systems. The DPO presented the four reports to the Executive Director according to the Implementing Rules on data protection approved by the Management Board. The other one is still in draft.
For the elaboration of the reports the DPO applied the policy and procedure for responding to Personal Data Breaches developed, approved and adopted in 2015.

2.1.5. Other procedures and policies

During the year of 2016, the DPO drafted a policy on data protection and another one on the access procedures for the supervisory authorities to exercise their powers at the core systems, which are very limited. However, the DP policy will be on hold as it will be adapted during 2017 to reflect the new regulation changes.
The DPO revised the PIA Procedure and drafted a PIA template in order to ease the work for any project managers when a PIA deemed to be required.

2.1.6. Opinion and Guidance

There are projects involving the processing operations on personal data where the DPO **is not requested** to provide any requirements or assessment, or, when rarely this is done, is at a late stage of the project where few or no changes are possible to make. This has been a recurrent situation.
In order to change this, the DPO enhanced a frequent monthly meeting with the Security Officer of the Agency and took the same approach by contacting the Head of Sector of Corporate Services but in this case, the request is still pending.

Regarding the consultation process on documents, which might have an impact on the processing of personal data at eu-LISA, they are frequently presented as final, without previous consultation to the DPO as required. Other cases the DPO is not even informed about, being completely ignored which is contrary to the obligations established by the Management Board Decision 93/2013, Article 6(5).
The DPO several times, in the Management Committee meetings, stressed the need to be consulted on matters that may have an impact on the compliance with the legal framework of processing of personal data by eu-LISA, without any visible or tangible effect.

The DPO is not part of the Change Management process, meaning that the DPO is not informed on changes to the systems, or very rarely is informed by Security. The DPO attended, when possible, to the meeting of the PMO in order to be acquainted with the status of the projects. However, the information provided in such meetings was not informative enough and in some cases did not reflect the real projects ongoing at eu-LISA aside the ones related with the large-scale systems, where the proper information was possible to be founded.

In the evaluation of the Agency[1], one of the requirements was:

> *"In collaboration with the DPO, the Agency's Management, Procurement and Legal Officers should ensure that appropriate data protection clauses are included in the agreements entered into with external contractors and for future service contracts."*

This is clearly not the case, as the DPO is not involved in such requirements or consultation process

[1] European Commission final evaluation report - "Independent external evaluation of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice – eu-LISA" – of March 2016.

2.2. Supervision by the EDPS and others

The following sections address the collaboration actions with the EDPS, Supervision Coordination Groups and others stakeholders with relevant work for eu-LISA.

2.2.1. Inspections by EDPS to core systems

The DPO acted as the pivot between eu-LISA and the EDPS on the preparations of the inspection held this year. The DPO was also involved with the comments phase on the EDPS VIS draft report, helping to harmonize and consolidate the comments made by eu-LISA to the report.

The DPO was also coordinating, upon empowerment of the Executive Director, the status of the recommendations made by the EDPS to the SISII Inspection Report of 2015. The EDPS, during the inspection to EURODAC requested the update on the status of the recommendations done in 2015 for the SISII.

2.2.2. Supervision Coordination Groups – Eurodac, VIS and SIS II

Following the legal requirement of Article 4(3) of the Implementing Rule on data protection, by invitation of the Supervision Coordination Group of SISII, Eurodac and VIS the DPO represented eu-LISA at the meeting. The group requested update information regarding the three scale-systems on operational matters. The SCGs' were interested on how the systems were performing, incidents related, roll-out status of VIS, Eurodac Recast status of play, quality of the data and information on the inspections. The meeting was held in March 2016.
The meeting organised in the fall of 2016, due to unavailability of the DPO, it was agree that the SCG's get only the information by e-mail.

2.2.3. DPO's Network meeting

During the months of April and October, the DPO attended the 39th and 40th DPOs' Network meeting. The themes addressed was the new regulation, the General Data Protection Regulation, the impact for the organisations, along with several practical workshops held by the EDPS to provide training and knowledge on best practices.
The next meeting will be organised by eu-LISA in Tallinn on the 31st May and 1st June 2017.

2.2.4. Collaboration with other entities

- In May, the DPO was invited to chair a panel on the EUROPOL conference addressing encryption and privacy;
- In July the DPO hosted a meeting with the EUROPOL's DPO, upon the cooperation Memorandum of Understanding establish between the two agencies. The discussion addressed the strategies on common interest topics;
- In July, the DPO participated actively in the Security and Privacy week 2016 with contribution to the discussions upon invitation;
- In August, the DPO was invited by BEREC's DPO in order to explore future close cooperation due to the proximity location;
- In September, the DPO was invited by ENISA to be part of a discussion panel in the Annual Privacy Forum 2016 sponsored by ENISA, Goethe University and DG Connect;
- In September, the eu-LISA's DPO was invited by the European Association Biometrics to participate in the conference were the recent technologies in the biometric research was presented. Taking this opportunity the DPO in the bi-weekly newsletter, issued a special edition addressing only biometrics technologies, recent developments;
- In November the DPO, upon the MoU established with Frontex, made a visit providing contribute to the Frontex staff awareness session on personal data. In the same visit it was exchanged best practices among DPOs and addressed the theme on common problems;
- In November the DPO was invited, as also a frequent member, to participate on the International Working Group on Data Protection on Telecommunications, the so known as the Berlin group;
- In November the DPO was invited as a speaker, by CEPOL on the Webinar – 77/2016 Data Protection and Handling/Processing of personal data according to the EU Legislation – addressing the work of eu-LISA in terms of Data Protection compliance to an audience of around 200 participants;

2.2.5. JHAA DPOs Meeting

On 29 November 2016, upon an initiative of the DPO, eu-LISA hosted the first meeting of the Justice and Home Affairs Agencies' Data Protection Officers (hereinafter referred as to "JHAA DPOs") in Tallinn.
This meeting was held aside of the DPO network gathering all the DPOs of the European Union Institutions and bodies (currently: 65 different entities) because it focuses on the daily working routine of JHAA DPOs. JHA Agencies provide operational structures to secure the European Union territory and faces identical problems as they deal with highly sensitive issues.
The main purposes of establishing a JHAA DPO working sub-group are to:

- Enhance the collaboration and the cooperation amongst DPOs working in JHA Agencies;
- Create a place for discussion regarding operational issues that JHAA DPOs encounter;
- Exchange best practices and views in order to improve the working method of each DPOs within their own Agencies;
- Share experiences and learn from each other in order to contribute, in the best way possible, for the JHAA DPOs daily work;
- Involvement of the DPO in early stages of any project of the organisation;
- Involvement of the DPO in the Governance model of the organisation. The DPO is a partner and a knowledgeable expert contributing for the excellency of any JHA Agency.

2.3. SISII, VIS and Eurodac – Opinion and guidance

The DPO was involved on the project about data quality reports for SISII. The initial procedure considered relevant by eu-LISA, MSs in the SISII Advisory Group and COM, received a negative opinion by the EDPS, on the basis that eu-LISA does not have the legal basis in the Regulation to carry out this reporting process. Following a negative opinion by the Supervisory Authority for the SISII, the DPO prepared and presented to the Executive Director a solution in order to accommodate the requests of the MSs, and be also legal compliant.
This also proofs that Data Protection is a partner seeking for solutions and not creating hindrances as it is in many cases, perceived.
The DPO have raised also doubts about the efficiency and effectiveness of such reports, as the quality of the data should be assessed at the time of the inserting the record and enforced by technically measure, not using patch solutions that already proven inefficient. The DPO already expressed his view in internal meetings, when invited, about how to tackle and mitigate the quality of the data on the systems.
In fact, it was verified that the current technical rules upon the insertion of data on some systems, do not comply with the regulation that rules the system, but this was the choice of the member states at the time of the design and implementation of the systems. The relaxation of the technical rules in this cases leads that incomplete data is inserted on the systems against the legal framework. The EDPS already expressed this problem upon the assessment of eu-LISA on creating the quality reports.

On other requests to produce statistics or run queries on the core systems, the DPO provided the opinion, when it is requested and when knows about the request, that eu-LISA does not have legal basis to run such queries. The role of eu-LISA is of management authority of the systems, as such, cannot act as a controller of the data for producing statistics or any kind of reports, out of the legal

framework, by accessing to the personal data held by the core systems, as this was stressed also by the EDPS.

Addressing the role on the large scale systems (core systems), the DPO already raised some concerns both to the EDPS inspections teams and to the Executive Director. **The DPO would like to be clarified the role towards to the core systems, because the current implementing rules do not expressly address the powers or role of the DPO on the core systems**. The DPO does not know if he can have access for example to the logs of the core systems, as this task is entrusted to the EDPS and National Data Protection Authorities. However, in some recent exchanges of opinion with the EDPS team and also on the recommendations of the inspection reports, the EDPS stresses the need for the DPO to be involved in the monitoring of the legal compliance of the core systems towards the processing of personal data.

2.4. Publications and policies

In March, the DPO produced the report on the annual work of 2015 presented to eu-LISA Management Board.

The publication of a bi-weekly newsletter is being issued as planned and in 2016, 20 were produced. The aim of the newsletter is to inform the eu-LISA staff about the recent developments on the data protection field, in special the new Regulation and national laws. The newsletter intends to inform also on security issues related with personal data and this is a way to create and raise privacy and protection of personal data conscience awareness. The DPO tries that the themes of interest for eu-LISA are the main topics.

The DPO revised and updated the Service Catalogue accordingly for the year 2016 and the internal business processes were mapped accordingly.

The DPO also developed with the collaboration of the HRT Unit Training Officer a specific module for newcomers on Data protection at eu-LISA.

The DPO created the space for data protection on eu-LISA website. This can be consulted in the following link:
http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/DP/Pages/default.aspx

The DPO also started to update regularly the eu-LISA DPO intranet page, where the recent topics are publish.

2.5. Complaint procedure

As part of the objective, the DPO developed a public complaint procedure where any person can address a complaint to the DPO. It provides guidance and clarifies that in case the complaint is related with one of the core systems, how to re-route the complaint in an efficient way.
The procedure and complaint mechanism is available in:
http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/DP/Documents/Complaint%20Procedure.pdf

The data subject rights section and how to complain is available in the following link:
http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/DP/Pages/DS-Rights.aspx

3. Conclusions

The level of compliance with the Regulation is progressing but there is still room for improvement. However, the lack of perception from managers and the need to comply with the data protection legal framework can create obstacles to close the gap by undermining the work of the DPO.

The DPO expects that the situation regarding the involvement on an early stage on projects addressing processing operations with personal data, will change in a near future along with the proper consultation timing on relevant documents such as contracts, that may have an impact addressing processing of personal data.

One of the main problems is the need to have a proper representation in Strasbourg site as the EDPS already recommended in 2015 along with the Report on the Evaluation of the Agency. This lack of representation in the operational site creates a critical gap in terms of information with the state of play of the core systems. Allied to the lack of resources can in fact create the misperception that the DPO does not provide guidance or feedback in due time, just because of the workload.
The representation in Strasbourg is also linked to the role that is expected in terms of monitor the compliance towards the legal framework of the core systems and the Implementing Rules. Nevertheless, the Regulation 45/2001 applies to the all set of regulations, which can bring some clarity to the role of the DPO.The lack of proper resources, already transmitted since 2014, to the Executive Director under the bi-lateral meetings, but never solved, is a recurrent topic of the reports to the eu-LISA Management Board.

Glossary on definitions

Symbols and abbreviated terms	Definitions
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
HRT Unit	Human Resource and Training Unit
IT	Information Technology
PIA	Privacy Impact assessment - systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing privacy risk
PMO	Project Management Office of eu-LISA
PII	Personally Identifiable Information
Risk	in a privacy context, a risk can be more precisely defined as the impacts of potential events on PII principals' privacy, and is characterized by its level of impact and its likelihood
Stakeholder	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
SCG	Supervision Coordination Group