Annual Work Report - 2014

Data Protection Officer

Table of Contents

1. Introduction

On the 23 December 2013 the Management Board of eu-LISA adopted 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.
The monitoring of lawfulness of the processing of personal data in conformity with data protection guidelines is guarantee at a first line by the eu-LISA Data Protection Officer (DPO) and in a second line with the role of supervisory the European Data Protection Supervisor (EDPS).
The DPO is required to transmit an annual report on the situation regarding the protection of staff and non-staff with regard to the processing of personal data in eu-LISA to the Management Board.
The following sections transmit the work of the DPO during the last 9 months of 2014.

2. Work report

On the 17th March 2014, the DPO took position at eu-LISA in order to monitor the application and compliance of the Agency with the Regulation along with the approved implementing rules. Until that moment, the DPO role was ensured by the Security Officer.
The first steps taken were to address the organisation of the work and attend the critical needs on personal data protection compliance. The roadmap of actions was also presented and agreed with the Executive Director in July 2014.
The DPO intended to implement regular meetings with key Heads of Units in order to address any specific topics from that unit with regards to personal data protection compliance, mainly: Security Officer, Executive Director, Head of Human Resources and Training Unit.
The only one not successful is with the IT Department (corporate) just because there are no Corporate IT department besides the core business services that eu-LISA provides.

2.1. Application Regulation 45/2001

The application of the regulation requires intensive work for raise the awareness of the staff as regard to the data protection compliance.

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 period between May and November 2014, the DPO made the following awareness sessions:

- 3 data protection awareness sessions;
- 3 data protection awareness sessions specific for IT staff;
- 1 awareness session training specific to HRT Unit;
- 3 training sessions on how to fill the DPO notification form;
- 2 sessions for management about Data protection in the projects and in the Units.

The privacy and processing of personal data notion consciousness is something that still lacks at staff level. The principle of need-to-know is still used only when convenient but in some cases not respected.

Regrettably, due to the low audience on the sessions proposed, it is foreseen to be mandatory sessions in the year 2015 monitored by the attendance list. The DPO plans for the next years to invert this tendency, fighting for the creation of a privacy awareness culture.

2.1.2. Notification and Register process

The notification of processing operations is a legal requirement both from the Management Board implementing rules as also from the Regulation.
One of the critical identified processes was to build the notification and inventory of the processing operations of the Agency.
A certain degree of consistency exists in relation to the categories of operations which are unlikely to affect adversely the rights and freedoms of the data subjects. They include data processing in relation to payroll management, accounting, partners and shareholders, customers and suppliers, HR data, etc.
One of the functions of notification is to inform the eu-LISA staff and others data subjects about existing processing operations by means of the public register of processing operations. The DPO considers it very important to make the register easily accessible to the staff and other data subjects.

The DPO notification form was concluded on the 16th September 2014 and the corresponding workflow needed to notify is also available – Annex 1. The workflow design allows understanding the information flow for register a processing operation with personal data.
The information 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 euLISA folder "19 Data Protection".

This notification form and all the inherent process was developed by the DPO.

Despite several presentations that were made to instruct the staff how to fill the DPO form and a specific addressed one in the management retreat, there are still a very low number of notifications presented to the DPO. By the end of 2014 only 9 notifications were presented to the DPO.

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 report is estimated to be completed by end of first quarter of 2015.

This survey with resemblances to an audit, helped to identify gaps and orient needs targeting the processing of personal data in the HRT Unit. Specific outcome of the survey was the effort and work developed by the unit in order to comply with the Regulation
A good outcome of the survey was the effort made by the HRT Unit to notify the processing operations identified.

2.1.4. Data Breaches

Regarding the Data Breach procedure handling, the DPO started to develop the procedure and the notification form on Personal Data Breaches – Annex 2 represents the workflow process.
During the year of 2014 the DPO carried out a data breach investigation and the report was produced and presented to the Executive Director according to the rules.

2.1.5. PIA Procedure

The PIA template was developed and presented to the PMO. However, the document was not well understood by the projects managers, also because it was much detailed for addressing the risks on processing personal data. The notion of risks in processing personal data is quite recent although the concept is included on the new foreseen Data Protection reform package.

The DPO will go to revise the document with the PMO comments and opinions made in order to improve the document in harmonised language of privacy, project managers and IT.
This is a recurrent situation, when dealing with processing of personal data. Each area have they own competences and the DPO recognizes that, besides the PIA template was developed according to recent standards and ISO, the DPO will develop into a low level easily to be understandable.

2.2. Service Catalogue

The Service Catalogue of the DPO was produced and presented to the Executive Director by end of June 2014. This Service Catalogue is a much granular catalogue of the services than the ones

represented in the corporate catalogue. This catalogue allows to the relevant stakeholders to identify the services provided by the DPO.

2.3. Opinion and Guidance

When consulted the DPO provided opinion about compliance of the data protection into projects under development by eu-LISA or one of the many contractors. Special relevance to projects like: Document Management, Allegro, Website (with the privacy notice), Multi Spectrum Image project on Fingerprints, among a lot of other miscellanies.
Several opinions were issued addressing the Access to HRT folders, on Accessing folders in the Network-attached Storage (NAS) and to the Internal Audit Charter. The recommendation made aimed to reduce and mitigate some risks identified for the protection of staff personal data.

2.3.1. Opinion and Guidance for SIS II/VIS and Eurodac

Another challenging area that the DPO face is the legal compliance of the systems we run. Each system has its own regulation, technical architecture, stakeholders, one supervisor, different controllers and co-controllers. This mixture of different scenarios presents complex data protection compliance with the technical compromise.
Very often, a simple technical solution cannot be implemented due to the complex data protection legal framework of the system. This is something not very well perceived by the different actors because is difficult to understand the unfavourable opinion of the DPO, that will require an extra effort, not efficient and in some cases under performant. Unfortunately or not those are the rules that we need to comply and rules are required as opposite to anarchy. Exceptions are created and permitted under supervision authorization.
Exceptional scenarios, which were not foreseen by the legislator, need to be assessed and solutions found. Those solutions must be found under the legal framework and with the knowledge of the main stakeholders, the Member States and the supervision authority for eu-LISA in terms of data protection compliance - the EDPS. The DPO at eu-LISA in those cases works as a translator between the eu-LISA technical language and the EDPS legal language.
During the year of 2014 the DPO provided a lot of opinions and guidance mainly in reaction mode for the SIS II, VIS/BMS and Eurodac.

The DPO had contributed on providing guidance for decommission of the old Eurodac system. Specific guidance was provided in order to destroy and guarantee the sanitization of the data on the Luxembourg Eurodac data center.
Certain requisites were needed to attain, in order to assure the compliance with the relocation of the data. The eu-LISA DPO in cooperation with the Security team issued several requirements that were needed to ensure in order to mitigate the risk for the transfer of personal data held by the system to the new location. The relocation was a success project not only from the operational side but also

from a data protection compliance side.

2.3.2. Opinion and Guidance for Smart-borders pilot

The DPO besides a small discussion with the contractor of Smart Borders, did not take any active participation on this project as it was not foreseen the processing of personal data by eu-LISA. However, it continues informing the EDPS about recent developments whenever this information is communicated to the DPO.

2.4. Meetings attended at European and International level

The DPO attended several meetings at European and International level, in order to participate and discuss the latest trends at technological level and legal aspects on privacy and processing of personal data.

2.4.1. Meetings with the Supervisory Authority

The DPO had a meeting with the EDPS in April and hosted one in November 2014. These meetings served to align expectations and establish future collaboration between the two. In the visit of November 2014, the EDPS made several presentations and awareness training on personal data protection, regrettably due to clash of agenda it was not possible to meet with management.

2.4.2. Meetings with the SISII, VIS and Eurodac Supervision Coordination Groups

The SCG's is composed by the National Data Protection Authorities and the EDPS, representing the roles of supervision authorities for the national systems and the as the authority for the management authority respectively.
Regarding the meetings of the Supervision Coordination Group of SISII, VIS and Eurodac, the DPO represented eu-LISA at the two meetings held yearly. Normally on these meetings it is required to inform the group about the latest issues and developments of the systems that may impact the processing of personal data.
The latest letter from the VIS SCG to eu-LISA emphasizing the high level of expertise provided to the group by the eu-LISA's DPO is an example of the appreciation for the work provided to the groups.
.

2.4.3. DPO's Network

The DPO participated on the two meetings of the Data Protection Officers Network, where the theme of debate was the revision of Regulation 45/2001 and several exchanges of views on current topics with the EDPS.

2.4.4. Other meetings

The DPO also participated in a number of international meetings: eu-LISA Security Officers Network meeting, International Working Group for Data Protection in Telecommunications and Internet Privacy Engineering Network Workshop.

2.5. Miscellaneous

In June 2014, the DPO obtained the certification as Data Protection Officer by EIPA. This is one of the certification advised by the EDPS for the role of a DPO in the EU institutions.

The DPO is leading the organisational preparations for the announced inspection to SISII by the EDPS that is foreseen for the end of February 2015. The DPO prepared the organisational information in order to address the doubts arising from managers on the mandate of the EDPS.

3. Conclusion

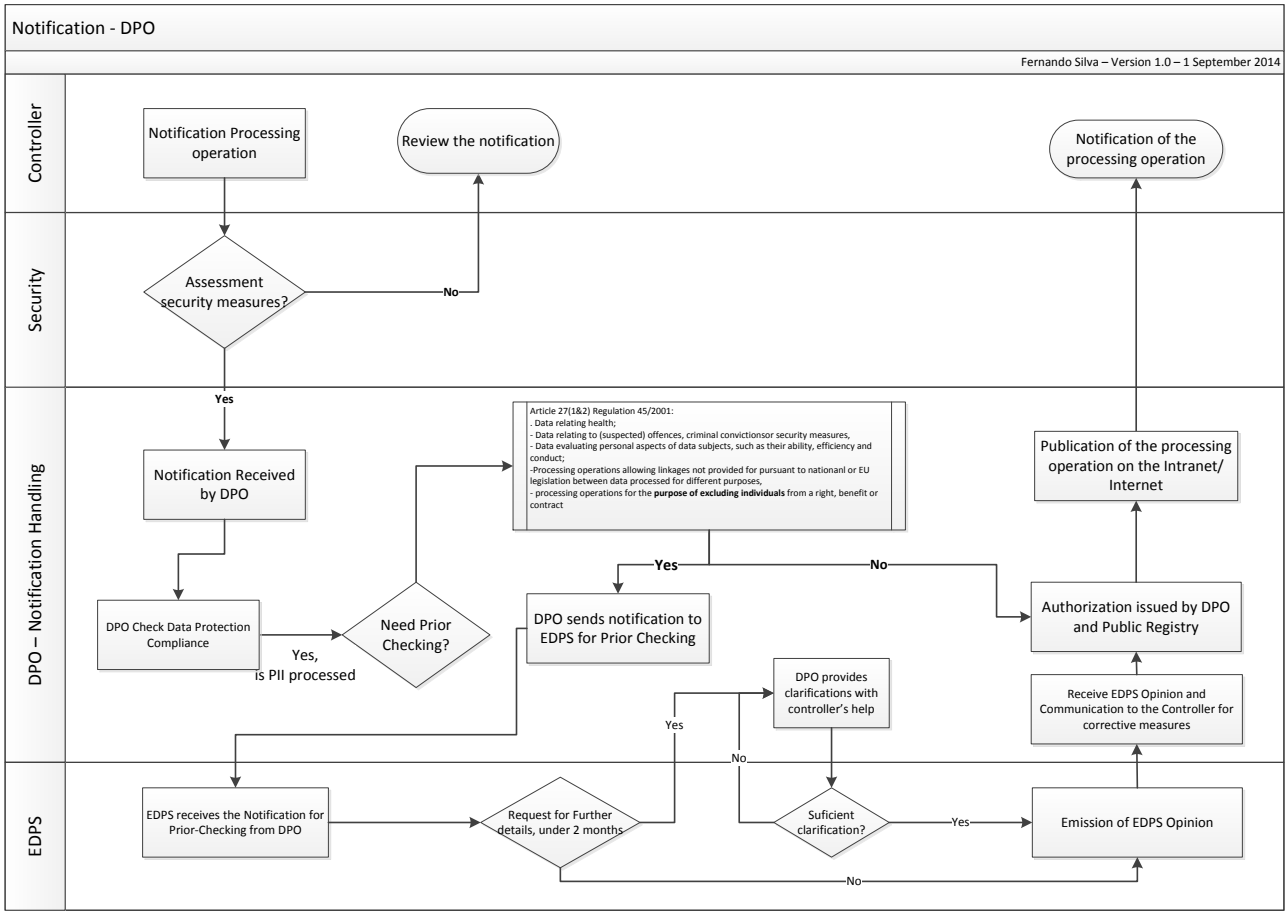
The main conclusion for the first nine months of work as DPO reveals that mainly is being hindered by a lack of operating resources, in particular administrative support and even by the distance with the operational data of the large systems. Although feeling support from the Executive Director, the DPO is aware that these needs will be addressed in due time.
In addition, the DPO needs more efficient communication tools and also being involved on the projects processing personal data in an early stage effectively and not just as a tick in a form as most the cases happen. Improved communication tools would certainly increase the visibility of the work and actions carried out.
More personal data awareness sessions must be performed in a mandatory regime. The personal data compliance does not raise the excitement as other themes, but it is required the knowledge when processing personal data since it is a core business for eu-LISA.

The DPO is committed in raising the data protection compliance taking into consideration that also depends a lot on the support of the management.

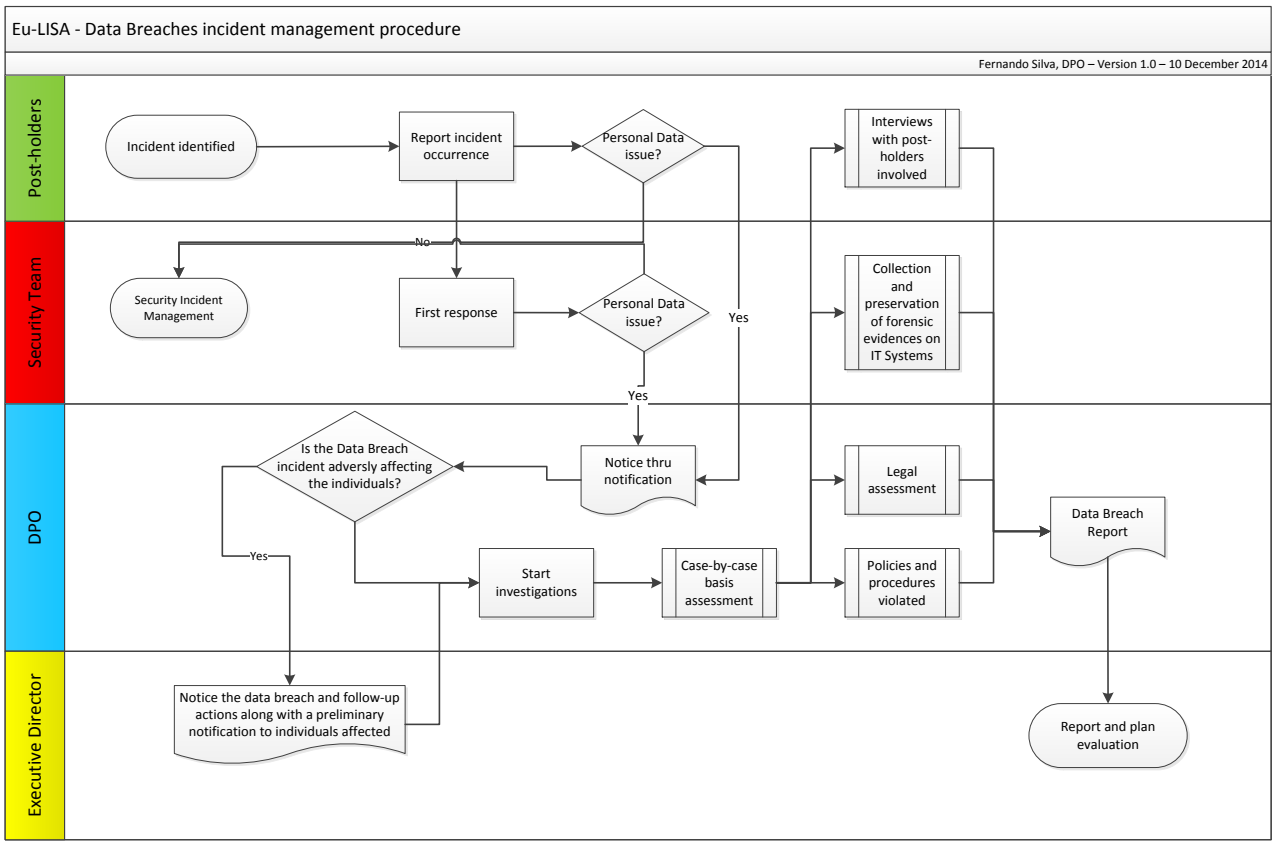
Glossary on definitions

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 Technologie
PIA	Privacy Impact assessment - systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, 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

ANNEX 1


Notification - DPO
Fernando Silva – Version 1.0 – 1 September 2014
Controller
Security
DPO – Notification Handling
EDPS
Notification Processing operation
Review the notification
Notification of the processing operation
Assessment security measures?
No
Yes
Notification Received by DPO
Article 27(1&2) Regulation 45/2001:
. Data relating health;
- Data relating to (suspected) offences, criminal convictionsor security measures,
- Data evaluating personal aspects of data subjects, such as their ability, efficiency and conduct;
-Processing operations allowing linkages not provided for pursuant to nationanl or EU legislation between data processed for different purposes,
- processing operations for the purpose of excluding individuals from a right, benefit or contract
Publication of the processing operation on the Intranet/ Internet
Yes
No
DPO Check Data Protection Compliance
Yes, is PII processed
Need Prior Checking?
DPO sends notification to EDPS for Prior Checking
Authorization issued by DPO and Public Registry
DPO provides clarifications with controller's help
Receive EDPS Opinion and Communication to the Controller for corrective measures
Yes
No
EDPS receives the Notification for Prior-Checking from DPO
Request for Further details, under 2 months
Suficient clarification?
Yes
Emission of EDPS Opinion
No

ANNEX 2


Eu-LISA - Data Breaches incident management procedure
Fernando Silva, DPO – Version 1.0 – 10 December 2014
Post-holders
Security Team
DPO
Executive Director
Incident identified
Report incident occurrence
Personal Data issue?
Interviews with post-holders involved
No
Security Incident Management
First response
Personal Data issue?
Yes
Collection and preservation of forensic evidences on IT Systems
Yes
Is the Data Breach incident adversly affecting the individuals?
Notice thru notification
Legal assessment
Data Breach Report
Yes
Start investigations
Case-by-case basis assessment
Policies and procedures violated
Notice the data breach and follow-up actions along with a preliminary notification to individuals affected
Report and plan evaluation