2016-037

From: Fernando Silva, Data Protection Officer

To: eu-LISA Management Board

Subject DPO Annual Work Report - 2015

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 - 2015

Data Protection Officer

Table of Contents

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:	28/02/2016

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*22/02/2016*	DPO	Initial version of the document created
[2]	*28/02/2016*	DPO	Revision

Configuration Management: Document Location

The latest version of this controlled document is stored in \\nas-tll\eulisa\19 Data protection folder on the NAS.

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").
Decision 93/2013 sets the data protection principles and rules applicable to eu-LISA as well as clarifies role and tasks of the Data Protection Officer (DPO) in regard to the monitoring and supervising of those rules and principles.
On one hand the eu-LISA DPO shall monitor and ensure that the provisions laid down in the Regulation are applied by eu-LISA, on the other, 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. This report illustrates how the DPO monitored and ensured eu-LISA compliance with Regulation during the year 2015.

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 2015 in relation to monitoring and ensuring compliance at eu-LISA with Regulation 45/2001 and will assess the current 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 2015, the DPO held the following awareness sessions:

- 5 general data protection awareness sessions;
- 1 awareness session training dedicated to the processing operations carried out by the HRT

Unit;

- 1 data protection awareness provided by the EDPS to the staff;
- 1 data protection awareness session dedicated to eu-LISA staff Management about data protection compliance.

The privacy and processing of personal data consciousness is something that still lacks at staff level. The principle of need-to-know is used only when convenient and in some cases even not respected. Despite the DPO organized the awareness sessions in advance and with due notice both for eu-LISA Tallinn and eu-LISA Strasbourg staff, this year attendance was lower than the forecast. Low attendance was registered also for the EDPS awareness session organised in eu-LISA Tallinn premises (in video-conference connection with eu-LISA Strasbourg). However, it has to be mentioned that in that occasion the staff of eu-LISA Strasbourg could not manage to be present at the event since they were performing the teambuilding.

The use of external contractors, the so-called "*intra-muros*" also creates hindrances as the DPO notices in some cases a total absence on Data Protection principles as also some lack of commitment to participate on the awareness session as they are for the staff. For the year 2016 the DPO intends to close this gap with awareness sessions targeted for non-eu-LISA staff but performing tasks on a daily base dealing with personal data.

Furthermore 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 is planning to design and develop some interactive material as an induction phase for newcomers.

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 Management Board implementing rules and under the Regulation.
The DPO noted a very high resistance on notifying processing operations on personal data, whether by the workload that the staff in the Agency is subject to, whether by the lack of commitment towards the legal obligation, whether by the lack of interest or even information on the obligation to notify, however the behaviour does not change even after the DPO reminds about it and after awareness sessions. On the last quarter of 2015 the DPO noticed more commitment from the managers in order to close the gap between the inventory and the register.
The DPO has been working closely with units and staff that manifested real interest in seeking guidance in complying with the Regulation.
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 eu-LISA folder "19 Data Protection".

At the end of 2015, 37 processing operations with personal data were notified to the DPO, 24 presented during the year, 5 required prior-checking to the EDPS.
Currently 51 processing operations have been identified by the DPO revealing a difference of 27% between the register and the inventory.

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. Due to the numerous changes in the Unit some of the recommendations are no longer valid for the Unit. The DPO agreed with the Head of HRT Unit to rewrite the report to reflect the current situation on the Unit and incorporating the comments made.
Due the primary assessment of the survey report, HRT Unit made efforts to mitigate immediately most of the recommendations related with the need for notification the processing operations, which some of them required prior-checking to the EDPS.

2.1.4. Data Breaches

During the reference period for this report, the DPO investigated four data breaches and three of the resulting reports were submitted to the Executive Director.
The DPO developed the policy and procedure for responding to Personal Data Breaches. This policy was formally approved and adopted in November 2015.

2.1.5. Other procedures and policies

During the year of 2015 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. Such documents are in drafted version and it is foreseen to be worked and finalised during the year of 2016.

2.1.6. Opinion and Guidance

The opinion of the DPO was requested several times by the staff in order to investigate possible

breaches of the provisions of the Regulation. In most of the cases the DPO concluded that there were violations and issued opinions and recommendations in order to address such breaches. The DPO however wants to highlight that most of those assessments were not possible to conclude in a due timeframe as a result of overload and lack of resources that the DPO is facing.

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. Projects such as the new electronic application for HR, SharePoint project, ICT Corporate projects, just to mention a few of those where the involvement of the DPO was done at a later stage or not even considered.

Regarding the elaboration of 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. In some 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). In the Management Committee meetings, the DPO stressed several times without results 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.

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 two inspections held this year. There was an inspection, by the EDPS, to the SIS II in February 2015 and a second one to the VIS System by the end of September 2015.
The DPO along with the relevant parties of eu-LISA, with special thanks for the Security team, prepared all the requested documentation, organised the inspection and post-documentation requests that was held in Strasbourg.
During the inspections the DPO was always present to support the eu-LISA interviewed staff and providing the relevant clarifications when required.
The DPO was also involved with the comments phase on the EDPS SIS II draft report, helping to harmonize and consolidate the comments made by eu-LISA to the report.

2.2.2. EDPS Visit

By invitation of eu-LISA's Executive Director, the EDPS, Mr. Giovanni Buttarelli made a visit to Tallinn headquarters where relevant themes for eu-LISA were discussed. During that visit, the EDPS also had a meeting with the DPO and organised session awareness to the staff on data protection.

2.2.3. 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 (SCG) of SIS II, Eurodac and VIS the DPO represented eu-LISA at the meeting. The group requested updated information regarding the three scale-systems on operational matters. The SCGs were interested in 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 meetings were held in March and in October 2015.
On 22 September a small group of representatives of the SCG Eurodac and EDPS visited the eu-LISA datacentre in Strasbourg, where they had a meeting with the scope to get acquainted with the architecture of the three systems and also with the physical site. The group was very impressed with the work of eu-LISA as also presented all the support to the work of the eu-LISA DPO during the SCG meeting in October 2015.

2.2.4. DPO's Network meeting

During the month of May the DPO attended the DPOs' Network meeting. eu-LISA's DPO was invited to make a presentation about "Security Incidents Reporting" where he presented the best practices on how to investigate data breaches and why a DPO should have an active role on security incidents. After the meeting it was requested by the DPOs present to share the Data Breaches Policy developed for eu-LISA.

2.2.5. Collaboration with other entities

In May contacts were established with the Estonian National Data Protection Authority by inviting a representative commissioner to visit the premises of eu-LISA and seek guidance on compliance with the national law regarding the video surveillance on the exterior which is not under direct responsibility of eu-LISA.

In September eu-LISA's DPO was invited by the European Association for Biometrics to chair a panel debate addressing the theme "A new perspective on Privacy and Biometrics with the new EU Regulation".

In October the DPO participated in the 58th International Working Group on Data Protection and Telecommunications, held in Berlin where topics related with biometrics, security of the telecommunications, authentication methods, and recent trends threating the right to privacy were discussed.

2.3. SISII, VIS and Eurodac – Opinion and guidance

The DPO has been involved in the projects about data quality and data Amnesty reports both for SIS II. In April the DPO participated in a workshop organised by eu-LISA in order to explain to the Member States (MSs) the arguments and the legal basis that the EDPS used when requested to eu-LISA to stop any reporting project on Data quality of the SIS II. By that time it was requested by the MSs and Commission for the DPO to draft a document to entrust eu-LISA to proceed, under the support and formal request of the MSs, with the project. The document was prepared in May and sent for consultation with the chair of the SIS II AG, which he approved. However, the whole process was put on hold, by request of the SIS II Application Management and the Executive Director, in order for eu-LISA to review the internal processes. By the end of September, there was a formal request by the SIS II Application Manager to proceed with the formal consultation to the MSs in order to entrust eu-LISA for carrying out the data quality reports. In the beginning of October a formal consultation was launched and by the end of October the approval was reached by the MSs at the SIS II AG. By the middle of November, in collaboration with the services of the Commission, a request for opinion was sent to the EDPS. The DPO presented the project as a functionality of the CS.SIS II system to provide the data quality reports and requested the opinion of the EDPS as the supervisory authority for eu-LISA. This procedure is considered relevant as according to the EDPS eu-LISA does not have the legal basis in the Regulation to carry out this reporting process.

Regarding the Amnesty reports of SIS II, the DPO made an assessment and provided an opinion which concluded that eu-LISA has the legal basis to produce such reports under the migration procedures established in the legal framework.

On other requests to produce statistics or run queries on the core systems, the DPO always provided the opinion that eu-LISA does not have legal basis to run such queries, since the role of eu-LISA is of management authority, as such, cannot act as a controller of the data for producing statistics or any kind of reports by accessing to the personal data held by the core systems.

2.4. Publications and policies

In March the DPO issued the report on the annual work of 2014, which was presented to eu-LISA Management Board.

In the beginning of October the DPO initiated the publication of a bi-weekly newsletter. The aim of the newsletter is to inform the eu-LISA staff about the recent developments on the data protection field, especially the new Regulation and national laws. The newsletter intends to inform also on security issues related to personal data and this is a way to create and raise privacy and protection of personal data conscience awareness.

The DPO also finalised a Data Breach Policy and procedure along with the notification form, in order to have a formal procedure and documented process when dealing with personal data breaches. This document is within the Management Committee for formal approval.

The DPO revised and updated the Service Catalogue accordingly for the year 2015 and the internal business processes were mapped accordingly.

3. Conclusions

As a general conclusion and comment is that the year of 2015 marks a transition period. The processes addressing the processing of personal data still need better assimilation by the managers and middle managers.
The level of compliance with the Regulation is still refining and there is room for improvement. The DPO believes that with small steps it is possible to achieve the goal. This goal is the commitment by management and staff with the need for compliance and respect with the Regulation.
This is the consequence of birth pains, the focus on critical and operational priorities and the workload that the eu-LISA staff is subject to.
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 that may have an impact addressing processing of personal data.
A continuous close contact with the staff and non-staff, by the use of the newsletter and other communication tools, by the awareness sessions, by creating initiatives to where the DPO can be regarded as a means that provides guidance and also solutions is in fact a long-term strategy.

3.1. Main challenges for 2016

The use of external contractors, the so called "*intra-muros*" introduces challenges in terms of commitment with the rules established when processing personal data. It also may increase the risk of data breaches.

Close the gap between notified processing operations and the inventory. This requires commitment by middle managers on compliance with the Regulation. Due to the lack of resources by the DPO it is challenging to enforce the roadmap established to accomplish compliance.

One of the problems felt by the DPO is also the lack of proper resources, already transmitted to the Executive Director under the bi-lateral meetings, but never solved, along with the need to have a proper representation in the Strasbourg site. 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. This 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.

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