From: Fernando Silva, Data Protection Officer

To: eu-LISA Management Board

Subject DPO Annual Work report - 2018

Protection level **PUBLIC**

DPO Annual Work Report - 2018
Data Protection Officer

Table of Contents

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report 2018 – Report on the annual activities of the eu-LISA's DPO
Document Author:	POCAS DA SILVA, Fernando (DPO)
Revision Status:	Final
Issue Date:	29/10/2018

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*23/10/2018*	DPO	Initial version of the document created
[2]	*29/10/2018*	DPO	Final version

1. Introduction

On the 23rd of 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 (hereinafter "The Implementing Rules").
The monitoring of lawfulness of the processing of personal data in conformity with data protection guidelines is guaranteed by the eu-LISA Data Protection Officer (DPO) and in a second line by the supervisory role of the European Data Protection Supervisor (EDPS).

2. Scope

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 2018.

Exceptionally, due to the resignation of the DPO this report reflects the activity thru the year of 2018, as the activities of the current DPO, Fernando Silva, are foreseen to end by 22nd November 2018.

3. DPO activities and actions

The following sections will explain by topic the current situation about the personal data protection compliance level at eu-LISA pertaining to Regulation 45/2001.

3.1. Awareness

In order to raise awareness, the DPO organised during the year, the following sessions:

- 3 Sessions on the GDPR on the end of May covering: GDPR Explained, Major questions and what to expect, two were held in Strasbourg and one in Tallinn with videoconference participation to Brussels liaison office;
- 6 Awareness sessions on Data Protection in May, June, October and November covering: Data protection principles, DPO role, Data protection at eu-LISA, Data Breaches, Supervision Role (EDPS);
- 2 data protection awareness session upon the on boarding programme of EES;
- 1 specific session for Human Resources Unit on data protection;
- One video recorded addressing data protection concerns and explain the importance to be

part of the training provided to the Member States on the VIS system – reflecting a recommendation derived from a data breach;

This 11 physical data protection sessions reflects the importance of the theme on the administrative data but also, the operational data, although still with low attendance from the operational site.

3.2. Notifications

The number of notifications is growing, starting to reflect the maturity of the agency and on the need to cope with the legal obligations on properly notify the processing operations addressing personal data.
By the end of October 2018 the DPO had 96 processing operations notified, with 14 corresponding to the year of 2018. There is still room for improvement as some critical processing operations have not been notified despite the reminders of the DPO.
The prior-checking of several notifications was put on hold, following the recommendation of the EDPS, in order to align with the new Regulation requirements.

3.3. Personal Data Breaches

During the reference period for this report, the DPO investigated 5 possible data breaches and the reports were submitted to the Executive Director, in accordance with the Implementing Rules on data protection approved by the Management Board.
From this 5 investigations, 4 were related with the Core systems.

The DPO also revised the data breach policy and procedure, following a recommendation of the EDPS on the Eurodac inspection report 2017 in order to include that "operational" data from the core systems to be covered by the policy.

3.4. Projects and change management process

Is still recurrent the miss of consultation on the Business Cases but the involvement in early stages of the project has been changing. The DPO has been consulted on the following projects:

- VIS test database;
- Synthetic fingerprint biometric test database;
- SIS II transliteration project, although at a late stage;
- Ex-ante evaluation on two projects, but due to the poor quality of the business cases could not provide an informed opinion;
- E-recruitment module for HR Unit;
- Anaplan project;
- Several ones from Security Unit;

The DPO would like to make a remark that the business cases included a section where should be made a reference to the data protection issues that the possible project may have. This does not happen in the light business case template where there is no reason why this was omitted. Most of the business cases templates used, is assumed to be the light one, where no data protection assessment is required.

Since the Management Board requested the involvement of the DPO in the approval process of the Change Management procedure, the DPO provided during the refer period of this report:

- 327 assessment to the RFCs;
- 19 assessments to the RFCs requiring further explanations in order to be approved by the DPO;
- 7 were denied as the request was not compliant with the legal framework;

These assessments require a huge amount of time from the DPO and also constant monitoring in order not to create delays in the Change Management process which creates a problem as **the DPO does not have a backup person**.

3.5. Prior consultation on decisions and policies/procedures

Regarding the consultation process on documents that might have an impact on the processing of personal data at eu-LISA, the DPO noticed an improvement as has been duly consulted on the policies and procedures in a time manner. However, issues related with the reorganization of eu-LISA and in particular with the consultation on the resources needed the DPO was not taken into consideration, despite the need to address the lack of human resources for the DPO function.

3.6. Supervision and Collaboration

3.6.1. EDPS inspection and recommendations

The DPO acted as the pivot between eu-LISA and the EDPS on the preparations for the inspection to the Schengen Information System II and VISA system held in beginning of November 2018.
Due to the EDPS SIS/VIS inspection the DPO was requested to update and monitor the status of the recommendations for which was not the process owner.
For the Eurodac EDPS inspection recommendations, the DPO is monitoring the status of the recommendations issued.

3.6.2. Supervision Coordination Groups for Eurodac, SIS II and VIS

Following the legal requirement of Article 4(3) of the Implementing Rule on data protection, by invitation of the Supervision Coordination Group (SCG) of Eurodac, SIS II and VIS the DPO represented eu-LISA at the meetings. The groups, composed by representatives of the National Data Protection Authorities along with the EDPS, requested updated information regarding the three large-scale IT systems on operational matters. The SCG members were interested in how the systems were performing, in the related incidents, in the roll-out status of VIS, in the Eurodac recast state of play, in the quality of the data and in information on the inspections conducted by the EDPS to the large scale systems managed by eu-LISA.
The meetings were held in June and November 2018, due to the lack of human resources entrusted to the DPO, it was not possible to be present for the meeting in November 2018.

One of the difficulties felt by the DPO is the lack of information feedback received from eu-LISA's Operations unit in Strasbourg. Since the DPO is representing eu-LISA at the SCG of Eurodac, SIS II and VIS, this creates hindrances to the quality of the information transmitted. This also raises concerns about the proper monitoring of the large-scale systems, for **which the DPO cannot carry out, although the EDPS requests that this task be entrusted to the DPO**.

3.6.3. DPO Network

The DPO participated on the 43rd DPO Network meeting hosted by the EDPS. The main topic was the new Regulation repealing the 45/2001 and the need to have guidance issued by the supervisory authority on the topics like privacy impact assessment, contractual clauses and data breaches.

3.6.4. JHAAs DPOs Network

The fourth meeting was organised by the EIGE DPO were the new regulation repealing Regulation 45/2001 was one of the main topics along with the new systems that may have an impact on the operations of the JHAAs DPOs tasks, in particular the articles addressing operational data.
The fifth meeting will be organised by Europol on the last week of November, but due lack of replacement, eu-LISA DPO will not be represented.

3.6.5. Cooperation with other entities

- In February, the DPO upon invitation by ENISA chaired a panel discussion: *Security of personal data – a research perspective*, on the workshop organised in partnership with the Italian Data Protection Authority;
- In March, the DPO was invited by Science Faculty of the University of Oporto, to give a talk about experience as a DPO and also on the workshop about GDPR;

- In February and in June the DPO give a lecture on Privacy Impact Assessment and on Privacy-by-design and by default at the EIPA course on certification of DPOs;
- In April the DPO, to the Members of the SON meeting, provided an half-day session addressing the theme on GDPR and Directive 680/2016;
- In April the DPO participated on the 63rd International Working Group on Data Protection and Telecommunications;
- In May the DPO was invited to be a discussant on a panel "*Interoperability of Agencies and databases: The Security of the Union"* hosted by the European University Institute of the conference program "Information Sharing and European Agencies: Novel Frontiers";
- In June, upon an awareness session in Tallinn, the BEREC DPO participated on the session in order to collect best practices and mutual cooperation;
- In June the DPO was invited to participate in the ENISA Annual Privacy Forum 2018, for which it was only possible to attend the second day, due to agenda constrains. As the IPEN meeting was also organised on the third day in the same city the DPO also participated on the IPEN Workshop 2018;
- In October the DPO participated on the International Conference Data Protection and Privacy Commissioners held in Brussels and sponsored by the EDPS under the topic "Debating ethics";

3.7. eu-LISA DPO Learning App

As part of the DPO strategy to cover all spectrum possible to reach eu-LISA staff and non-staff, to provide all sort of tools to be acquainted with the data protection legal obligations and data protection at eu-LISA a mobile App was developed and since September available.

This mobile app on data protection has been created for information and educational purposes by eu-LISA's Data Protection Office in collaboration with eu-LISA's Human Resources Unit.

The mobile app can be downloaded for free for mobile devices and addresses data protection at eu-LISA, provides some guidance, consultation on relevant pieces of legislation and receive news of the data protection world.

The purpose is to reinforce the high commitment of eu-LISA to the processing of personal data in a lawful way.

The eu-LISA DPO App allows:

- to deeply understand our commitment, by explaining all of our activities insofar as data protection is concerned;
- to consult the official legal texts regarding the processing of personal data, as well as other relevant documents;
- to keep abreast of the most varied developments related to privacy and data protection via our interactive news section.

The mobile App can be downloaded by searching Google store or Apple store with the key words: eu-LISA DPO, eu-LISA data protection, eu-LISA DPO.

For the Android devices, the App is available via the following link:

For the Apple iOS devices, the App is available via the following link:

It is also available via eu-LISA website: https://www.eulisa.europa.eu/Activities/Data-Protection/eu-lisa-dpo-app

3.8. Publications and policies

The following publications were issued or draft in cooperation by/with the DPO:

- DPO Annual Work Report 2017 – presented and approved by the eu-LISA Management Board;
- Conflict of interest policy – the DPO worked with eu-LISA Internal Auditor and HR Unit on drafting the policy according with data protection principles;
- Eu-LISA Video Surveillance Policy – The DPO along with Security Unit drafted the policy taking into consideration the EDPS Guidelines;
- Revision of the Teleworking Guidelines;
- Data Protection aspects in the application of the guidelines on Whistleblowing – HR Unit in close cooperation with the DPO drafted the guidelines;
- Data Protection Guidelines on Administrative inquires – drafted by the DPO;
- Data Breach Policy, Procedure, Form and Register – drafted by the DPO;

The publication of a bi-weekly newsletter is being issued as planned and it is already at its 65th issue, the last is dated from September 2018, that due to lack of resources along with the eu-LISA DPO App was suspended. The aim of the newsletter is to inform the eu-LISA staff about the recent developments in the data protection field, especially 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.
In 2018, 17 newsletters were issued.

3.9. Annual Survey

The annual survey to the GCU Unit planned for the year 2018 has been on hold due to the lack of

human resources and bandwidth from the DPO.

3.10. Repealing Regulation 45/2001

The action plan presented to the Executive Director and to the Management Committee was put in place, although a lot of the foreseen actions needed to wait for the final text as some grey areas need further clarification. The DPO made a gap analysis and the critical points were addressed as possible.

The DPO revised most of the privacy notices and updated accordingly with the cooperation of the owners of each process involved. However, when the final legal text became a reality and adopted, there is a need to proper revise the information.

4. Main challenges and risks

4.1. Lack of human resources

This is a section that does not change over the years. The DPO is still facing many problems with proper support due the **lack of administrative support and proper monitoring tasks in the Strasbourg site** as also stated by the Commission Evaluation of the Agency recommendation R.3.18[1]. The EDPS already communicated to the Executive Director in his letter of 22nd October 2015- C2015-0497, stressed also in the VIS Inspection Report of 2015-0507 recommendation 24, that the eu-LISA's DPO current situation, being based in Tallinn, while the agency's core business units are mostly located in Strasbourg, **is not satisfactory and should be reassess at least in terms of resources allocated.**

The DPO already reminded that **this situation is not compliant with the Implementing Rules,** Article 3.2[2]. The DPO is currently performing the tasks assigned with the support of an intern, which is manifestly insufficient for the tasks assigned.

With the resignation of the DPO, as communicated by letter in June to the Executive Director and to the Management Board, **there will be a period without this sensitive role being present at eu-**

[1] 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 – Final Evaluation Report, March 2016:
*"**R3.18** The Agency should enforce its data protection support in Strasbourg either by reallocating the DPO to Strasbourg or assigning a deputy DPO in Strasbourg to assist with data protection matters"*

[2] Article 3.2 of eu-LISA's Management Board Decision 2013-093:
"In accordance with Article 24(6) of the Regulation, the Data Protection Officer shall be provided the staff necessary to carry out his/her duties. The provisions on independence in Article 2(6) of this Decision apply to staff provided in support to the Data Protection Officers tasks and duties."

LISA, as there never was a backup person. This creates an increased risk of non-compliance towards the Data Protection legal framework.

4.2. New Regulation

The new Regulation repealing Regulation 45/2001 that is foreseen to enter into force by December 2018, will pose a challenge and bring added responsibilities to the EU Institutions and to eu-LISA in particular, due the accountability and need to demonstrate compliance.
For eu-LISA this will be quite challenging due the role as processor and controller, to the new systems and requirements to comply with the legal obligations in terms of data protection and the need to ensure the security of the processing of personal data operations within a more exposed environment.

5. Conclusions

The level of compliance at the Agency with Regulation 45/2001 improved a lot, in particular the consciences with the need to respect data protection principles and legal requirements. As always there is room for progress, in particular at the Strasbourg site where there is a notorious gap toward compliance compared with Tallinn and Brussels.

The DPO expects improvement in the following points:

- **Fulfilment of human resources needs for the DPO function**;
- The location of the DPO is a hindrance towards compliance with monitoring the Strasbourg site, which is expected to be changed with the allocation of proper human resources.

Glossary on definitions

Abbreviations, acronyms and 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
HoAMM	Head of Application Management and Maintenance Unit
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
EPMO	Eu-LISA Project Management Office Sector
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 organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity
SCG	Supervision Coordination Group