Protection level PUBLIC

Ares(2018)1040021

From: Fernando Silva, Data Protection Officer

To: eu-LISA Management Board

Subject DPO Annual Work report - 2017

Protection level	**PUBLIC**

DPO Annual Work Report - 2017
Data Protection Officer

Table of Contents

1. Introduction 4
2. Scope 4
3. DPO activities and actions 4
3.1. Awareness 4
3.2. Notifications 5
3.3. Personal Data Breaches 5
3.4. Projects and change management process 5
3.5. Prior consultation on decisions and policies/procedures 6
3.6. Supervision and Collaboration 6
3.6.1. EDPS inspection and recommendations 6
3.6.2. Supervision Coordination Groups for Eurodac, SIS II and VIS 7
3.6.3. JHAAs DPOs Network 7
3.6.4. Cooperation with other entities 7
3.7. DPO Networking meeting 8
3.8. Publications and policies 8
3.9. Annual Survey 8
3.10. Repealing Regulation 45/2001 9
4. Main challenges and risks 9
4.1. Lack of human resources 9
4.2. New Regulation 10
5. Conclusions 10
Annex - 41st DPO Network meeting, Tallinn, 31/05/2017 - survey 11
Glossary on definitions 18

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report 2017 – Report on the annual activities of the eu-LISA's DPO
Document Author:	POCAS DA SILVA, Fernando (DPO)
Revision Status:	Final
Issue Date:	22/02/2018

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*01/02/2018*	DPO	Initial version of the document created
[2]	*23/02/2018*	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 2017.

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, 8 sessions addressing the principles of protection of personal data, with eu-LISA post-holders.

For the Data Protection Day, the DPO organised two sessions held in Tallinn for the eu-LISA staff, while staff members in Brussels and Strasbourg could attend via the Video Conferencing system. A first session was held with Dr Dan Bogdanov addressing technology that implemented privacy by design preserving data privacy and a second session with Mr Andres Ojaver approaching data protection in a more informal, practical and operational way, with examples from public and private sector.

A special awareness session was provided to the GCU, explaining the aim of a DP Survey to the Unit and one session requested by the HoAMMU was delivered in Strasbourg to the AMM Unit. At the time, the DPO also booked two awareness sessions for Operations Unit with the attendance in total of 4 persons.

Taking advantage of the 41st DPO Network meeting held in Tallinn, two DPOs were invited to provide two sessions: one with the DPO of ECA, which addressed the theme of Security and Privacy by Design when processing personal data and the Commission's DPO, which addressed the role of the DPO within the EU Institutions.
During the year 2017, the DPO held the following awareness sessions:

- 8 general data protection awareness sessions, including Tallinn, Strasbourg and Brussels;
- 1 awareness session training dedicated to the annual survey for the GCU Unit.

3.2. Notifications

The number of notifications is growing, with a boost coming from the discussions with the Management Board and the concerns that some Head of Units demonstrated. The DPO notes still a very high resistance on notifying processing operations on personal data. One of the arguments for the lack of commitment by some units is the fact that the DPO is not known, at least at the Strasbourg site.
Currently the DPO has 89 processing operations in the inventory from which 82 are notified to the DPO and in the register.

3.3. Personal Data Breaches

During the reference period for this report, the DPO investigated one possible data breach and the resulting report was submitted to the Executive Director, in accordance with the Implementing Rules on data protection approved by the Management Board.

Upon a complaint lodged to the EDPS by one staff member, the DPO investigated two possible breaches with the legal framework and upon the request of eu-LISA's Executive Director, the DPO provided an opinion on another in order to reply to the EDPS. Two opinions were sent to the EDPS by the DPO on the facts alleged by the complainant, after an internal investigation. As a result, the EDPS issued some recommendations and closed the case. The other is are still pending the EDPS opinion.

3.4. Projects and change management process

The recurrent situation on projects involving the processing operations on personal data where the DPO **is not requested** to provide any requirements or assessment is improving slowly. The Security Unit is consulting the DPO on the projects they have, but apart from very few cases, the DPO was only consulted in three Business Cases from the AMM Unit, and the absence of involvement in early stages of the project is still the frequent situation. 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.
It is expected that for future this may change due the establishment of the EPMO sector and the revision of the Project Management procedures at eu-LISA.
The DPO was also involved in a workshop to address the unlinking methods at the Eurodac wrongly link establish between fingerprints.

Since the Management Board requested the involvement of the DPO in the approval process of the Change Management procedure, the DPO provided during the period from the end of February until December:

- 270 assessment to the RFCs;
- 27 assessments to the RFCs requiring further explanations in order to be approved by the DPO;
- 4 were required to change the scope in order to be compliant;

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. **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, it should be noted that they are frequently presented as final, without previous consultation to the DPO as required. In other cases the DPO is not even informed about them, being completely ignored, which is contrary to the obligations established by Management Board Decision 93/2013, Article 6(5).
In the Management Committee meetings, several times, the DPO 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.
One of the main reasons is the fact that the DPO is not part of the functional mailbox EULISA-Management, where some actors send the documents for consultation, which do not reach the DPO.
This process has not improved from last year's assessment.

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 of the comments to the Eurodac inspection report from last year, helping to harmonize and consolidate the comments made by eu-LISA to the report. Eu-LISA received the final EDPS Eurodac Inspection Report in

December 2017.
The DPO is not monitoring the status of the EDPS recommendations of the SIS II and VIS inspection reports.For the Eurodac, it has been agreed with the application Manager that the DPO will take ownership of the process on 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 2017.
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 raises concerns addressing the quality of the information transmitted to them. 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. JHAAs DPOs Network

Giving continuity to the first meeting organised by eu-LISA's DPO last year, the EMCDDA's DPO organised the second meeting, where topics like interoperability and new systems processing personal data were addressed.
The third meeting was organised by the Europol's 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.

3.6.4. Cooperation with other entities

- In March, the DPO had a meeting with the French DPA at the CNIL, inviting for the participation at the 41st DPO Network meeting but also addressing obligations of eu-LISA towards the location site in Strasbourg;
- In June and December 2017, the DPO was invited by EIPA to provide training to future DPOs at the Certification programme;
- In September, the DPO was invited by ISACA Bulgaria to participate and present the requirements imposed by the GDPR Regulation in the framework for protection of the information environment. On the following day was invited to moderate a panel about on meeting the requirements for the GDPR;

- In November the DPO attended the International Association Privacy Professionals (IAPP) where achieved the certification as Certified Information Privacy Manager (CIPM);
- In December the DPO was invited by EMA (European Medicines Agency) to participate in a workshop about data anonymization in order to share big data and be compliant with the GDPR;

3.7. DPO Networking meeting

The 41st DPO Network meeting was held in Tallinn and organised by eu-LISA's DPO. The number of DPOs from the EU Institutions participating was 75. A representative from the CNIL (The French Data Protection Authority, chair of the Working Party Article29), a representative of the DAPIX and a representative of the Estonian Ministry of Justice due the fact that will be chairing DAPIX during the Estonian EU Presidency were all invited to address the topics of interest. The EDPS organised the second day of the agenda, providing awareness training and information on recent developments in the area of the data protection.
The main theme was the proposal to repeal Regulation 45/2001 that will replicate the General Data Protection Regulation into a new Regulation applicable to the EU Institutions and Bodies from May 2018.
The DPO also decided to have workshops based on the proposed regulation on four main areas: DPO role, Accountability, Privacy Impact assessment and Privacy-by-design.
The first satisfaction survey held upon eu-LISA's DPO initiative, included as an annex to this report, gives a clear idea about the outcomes and provides way forward for future meetings.
In October the DPO attended the 42nd DPO network meeting organised by EMA, where a follow-up on the topics of the new Regulation was the main tone of the meeting.

3.8. Publications and policies

In March, the DPO produced the report on the annual work of 2016 presented to eu-LISA Management Board.
The publication of a bi-weekly newsletter is being issued as planned and it is already at its 48th issue. 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.

3.9. Annual Survey

The annual survey to the GCU Unit planned for the year 2017 had a kick-off meeting but has been on hold due to the lack of human resources and bandwidth from the DPO. The DPO might reassess this task in the future, taking into consideration the resources available.

3.10. Repealing Regulation 45/2001

In order to prepare eu-LISA for the new upcoming regulation that will replace the Regulation 45/2001, the DPO presented to the Executive Director, in November 2017, and to the Management Committee the action plan to ensure a smooth transition for the implementation of the new Regulation.

4. Main challenges and risks

4.1. Lack of human resources

The DPO is still facing many problems with proper support by **lacking 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.

Among the feedbacks provided by eu-LISA staff in Strasbourg is that the DPO is not known to the staff there nor do they know the DPO's function or role. As a remark, in the three years that the DPO is working at eu-LISA, 18 awareness sessions for Strasbourg were held. With the exception of the one mandatory for the HoAMM Unit, these sessions always had a very low number of participants.

---

[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."

4.2. New Regulation

The new Regulation repealing Regulation 45/2001 that is foreseen to translate the General Data Protection Regulation entering into force on the 25th of May 2018 will pose a challenge.
As stated in section 3.10, the DPO defined an action plan by evaluating the impact and proposing actions to mitigate the gaps.

5. Conclusions

The level of compliance at the Agency with Regulation 45/2001 is showing clear improvement with 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**;
- Proper timing consultation on relevant documents and projects that may have an impact addressing personal data;
- 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.

Annex - 41st DPO Network meeting, Tallinn, 31/05/2017 - survey

1. Organisation of the meeting

The meeting was well organised.

		Response Percent	Response Total
1	Strongly Agree	86.67%	26
2	Agree	13.33%	4
3	Neutral	0.00%	0
4	Disagree	0.00%	0
5	Strongly Disagree	0.00%	0

Analysis							
Mean:	1.13	Std. Deviation:	0.34	Satisfaction Rate:	3.33	answered	30
Variance:	0.12	Std. Error:	0.06			skipped	0

The programme was well-balanced (breaks, duration, sequence of topics)

		Response Percent	Response Total
1	Strongly Agree	63.33%	19
2	Agree	36.67%	11
3	Neutral	0.00%	0
4	Disagree	0.00%	0
5	Strongly Disagree	0.00%	0

Analysis							
Mean:	1.37	Std. Deviation:	0.48	Satisfaction Rate:	9.17	answered	30
Variance:	0.23	Std. Error:	0.09			skipped	0

The logistical arrangements were satisfactory (e.g. room facilities, coffee breaks, etc.)									
								Response Percent	Response Total
1	Strongly Agree							70.00%	21
2	Agree							26.67%	8
3	Neutral							3.33%	1
4	Disagree							0.00%	0
5	Strongly Disagree							0.00%	0
Analysis	Mean:	1.33	Std. Deviation:	0.54	Satisfaction Rate:	8.33		answered	30
	Variance:	0.29	Std. Error:	0.1				skipped	0

2. Content

I found the information provided during the meeting relevant to my work.									
								Response Percent	Response Total
1	Strongly Agree							66.67%	20
2	Agree							33.33%	10
3	Neutral							0.00%	0
4	Disagree							0.00%	0
5	Strongly Disagree							0.00%	0
Analysis	Mean:	1.33	Std. Deviation:	0.47	Satisfaction Rate:	8.33		answered	30
	Variance:	0.22	Std. Error:	0.09				skipped	0

I am satisfied with the Agenda topics discussed during the meeting.

		Response Percent	Response Total
1	Strongly Agree	53.33%	16
2	Agree	43.33%	13
3	Neutral	3.33%	1
4	Disagree	0.00%	0
5	Strongly Disagree	0.00%	0

Analysis								
	Mean:	1.5	Std. Deviation:	0.56	Satisfaction Rate:	12.5	answered	30
	Variance:	0.32	Std. Error:	0.1			skipped	0

The Workshops about the five topics of the GDPR was relevant and should be continued in future meetings.

		Response Percent	Response Total
1	Strongly Agree	60.00%	18
2	Agree	40.00%	12
3	Neutral	0.00%	0
4	Disagree	0.00%	0
5	Strongly Disagree	0.00%	0

Analysis								
	Mean:	1.4	Std. Deviation:	0.49	Satisfaction Rate:	10	answered	30
	Variance:	0.24	Std. Error:	0.09			skipped	0

I prefer Workshops rather than other methods (i.e. Conferences, Presentations, etc)

		Response Percent	Response Total
1	Strongly Agree	33.33%	10
2	Agree	40.00%	12
3	Neutral	20.00%	6
4	Disagree	6.67%	2
5	Strongly Disagree	0.00%	0

Analysis								
Mean:	2	Std. Deviation:	0.89	Satisfaction Rate:	25	answered	30
Variance:	0.8	Std. Error:	0.16			skipped	0

I learned from the contributions of other colleagues.

		Response Percent	Response Total
1	Strongly Agree	50.00%	15
2	Agree	46.67%	14
3	Neutral	3.33%	1
4	Disagree	0.00%	0
5	Strongly Disagree	0.00%	0

Analysis							
Mean:	1.53	Std. Deviation:	0.56	Satisfaction Rate:	13.33	answered	30
Variance:	0.32	Std. Error:	0.1			skipped	0

3. Sessions

The presentation of eu-LISA was informative and with relevant information.

			Response Percent	Response Total
1	Strongly agree		60.00%	18
2	Agree		26.67%	8
3	Neutral		10.00%	3
4	Disagree		0.00%	0
5	Strongly disagree		3.33%	1

Analysis								
	Mean:	1.6	Std. Deviation:	0.92	Satisfaction Rate:	15	answered	30
	Variance:	0.84	Std. Error:	0.17			skipped	0

The intervention of the CNIL was relevant and informative

			Response Percent	Response Total
1	Strongly agree		30.00%	9
2	Agree		36.67%	11
3	Neutral		23.33%	7
4	Disagree		10.00%	3
5	Strongly disagree		0.00%	0

Analysis								
	Mean:	2.13	Std. Deviation:	0.96	Satisfaction Rate:	28.33	answered	30
	Variance:	0.92	Std. Error:	0.17			skipped	0

The presence of the DAPIX and Commission representatives was of an added-value and informative

			Response Percent	Response Total
1	Strongly agree		40.00%	12
2	Agree		56.67%	17
3	Neutral		3.33%	1
4	Disagree		0.00%	0
5	Strongly disagree		0.00%	0

Analysis							
	Mean:	1.63	Std. Deviation:	0.55	Satisfaction Rate:	15.83	answered 30
	Variance:	0.3	Std. Error:	0.1			skipped 0

Speakers coming from National DPAs or relevant bodies should be invited more often.

			Response Percent	Response Total
1	Strongly agree		26.67%	8
2	Agree		36.67%	11
3	Neutral		33.33%	10
4	Disagree		3.33%	1
5	Strongly disagree		0.00%	0

Analysis							
	Mean:	2.13	Std. Deviation:	0.85	Satisfaction Rate:	28.33	answered 30
	Variance:	0.72	Std. Error:	0.15			skipped 0

4. General satisfaction

I am satisfied with the meeting as a whole:				
			Response Percent	Response Total
1	Strongly agree		66.67%	20
2	Agree		33.33%	10
3	Neutral		0.00%	0
4	Disagree		0.00%	0
5	Strongly disagree		0.00%	0

Analysis	Mean:	1.33	Std. Deviation:	0.47	Satisfaction Rate:	8.33	answered	30
	Variance:	0.22	Std. Error:	0.09			skipped	0

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