From: Encarna Gimenez, Data Protection Officer (DPO)

To: eu-LISA Management Board

Subject DPO Annual Work report - 2019

2020-054

Protection level **PUBLIC**

DPO Annual Work Report - 2019

Table of Contents

1 Introduction 4
2 Scope 4
3 DPO activities and actions 4
3.1 Awareness 5
3.2 Records of Processing Activities 5
3.3 Personal Data Breaches 6
3.4 Data Protection Impact Assessments (DPIA) 6
3.5 Projects and change management process 7
3.6 Procurement 8
3.7 Prior consultation on decisions and policies/procedures 9
3.8 Supervision and Collaboration 9
3.8.1 EDPS inspection and recommendations 9
3.8.2 Supervision Coordination Groups for Eurodac, SIS II and VIS 10
3.8.3 JHAAs DPOs Network 10
3.9 DPO Network meeting 10
3.10 Annual Survey 10
4 Data Protection Function 11

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report 2019
Document Author:	DPO
Revision Status:	Final
Issue Date:	27/02/2020

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*01/02/2020*	Intern to DPO	Initial draft
[2]	*27/02/2020*	DPO	Final version

1 Introduction

eu-LISA started 2019 with a new mandate set out in Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (hereinafter – 'eu-LISA Regulation').

Article 2 of eu-LISA Regulation states the objectives of the Agency. In particular, *the Agency shall ensure a high level of data protection, in accordance with Union data protection law, including specific provisions for each large-scale IT system*.

2019 also started with a new applicable data protection regulation, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereinafter – 'Regulation (EU) 2018/1725').

On 9 October 2019 the Management Board of eu-LISA adopted Decision 2019-185 REV 1 on the Implementing Rules concerning the Data Protection Officer (DPO) pursuant to Article 45(3) of Regulation (EU) 2018/1725 (hereinafter – 'eu-LISA DPO Implementing Rules').

eu-LISA DPO should advise controllers and processors on fulfilling their obligations. Application of the provisions of Regulation (EU) 2018/1725 is firstly ensured by the DPO of eu-LISA and, ultimately, by the supervisory role of the European Data Protection Supervisor (EDPS).

2 Scope

Following Article 7 (4) of the eu-LISA DPO Implementing Rules, the DPO shall submit to the Agency's Management Board an annual report on her activities and on the state of play as regards the data protection activities and compliance of the Agency.

This report presents the status of the data protection activities within the Agency and compiles the work performed by the DPO during the year 2019. It should be noted that, until the middle of 2019, the DPO tasks and duties were performed by the eu-LISA Acting DPO and, from June 2019, by the newly appointed DPO.

3 DPO activities and actions

The following sections detail by topic the state of play as regards the data protection activities and compliance of the Agency with Regulation (EU) No 2018/1725.

3.1 Awareness

In order to raise awareness on data protection, the DPO of eu-LISA makes use of different tools including general awareness sessions, one-on-one coaching sessions, weekly newsletter or the dedicated Data Protection Officer intranet.

In January 2019, the Acting DPO organised an awareness session to celebrate Data Protection Day. This session offered a general view on data subjects' rights, records of processing activities, data protection impact assessments, data breaches and the role of Data Protection Officer and the European Data Protection Supervisor.

On 24 May, a new training was provided on video-surveillance and data protection-related aspects. eu-LISA DPO also promoted training organised by EDPS which are open for all staff such as the four training sessions for Heads of Unit/Heads of Sector in 2019.

Furthermore, the DPO has provided one-on-one coaching sessions to specific staff when seeking advice and guidance of the DPO to comply with their obligations as data controllers under the new data protection Regulation.

Likewise, in order to ease and provide better support for the data controllers in documenting data processing operations, the 'Data Protection Officer' intranet was updated with templates and step-by-step instructions. Similarly, a new section was created in the DPO intranet on 'Data Beach To Do List' which explains in detail steps and actions to follow should a data breach occur.

In addition, other efforts to raise awareness go into the internal weekly eu-LISA Newsletter which is send out to all eu-LISA staff. This weekly newsletter includes a dedicated section on data protection that the DPO prepares. The purpose of this section is to update staff on the latest guidelines, available trainings and recent developments in the field.

3.2 Records of Processing Activities

In compliance with Article 31 of the Regulation 2018/1725, eu-LISA shall maintain a record of processing activities under its responsibility. According to Article 4(3) of the eu-LISA DPO Implementing Rules, the DPO will keep a central register of records of their processing activities.

Therefore, when delegated data controllers in eu-LISA want to start a new processing activity in eu-LISA, they document this processing activity as a new record and notify this new record to the DPO so the central register can be updated accordingly. Also, when an existing processing activity changes in some way, the data controller needs to update the documentation associated to that record and notify the change to the DPO.

Step-by-step instructions and templates on how to document records of processing activities have been prepared by the DPO to facilitate the tasks and obligations of the data controller.

By the end of December 2019, the **eu-LISA register of data processing activities** included **102**

records. Four of them were registered during 2019. The central register of processing operations is published on the eu-LISA website and is constantly updated.

3.3 Personal Data Breaches

Following obligations stemming from article 34 (6) of the Regulation 2018/1725, "*data controller shall document any personal data breaches*". According to Article 4 (3) of the eu-LISA DPO Implementing Rules, the DPO will keep a central register of records of data breaches.

During the reference period for this report, six data breaches were reported and documented by the data controller. The central register of data breaches is updated accordingly by DPO. The DPO also supported data controller with the assessment in accordance with the EDPS guidelines on data breaches. Regard was also given to conditions set out in article 34 and 35 of the Regulation 2018/1725 on notification to EDPS and communication to affected data subjects.

Reports of the data breaches were submitted to Executive Director and to EDPS when applicable.

3.4 Data Protection Impact Assessments (DPIA)

Following its new establishing Regulation, eu-LISA is mandated to ensure a high level of data protection. On the other side, eu-LISA shall follow the principles of privacy by design and by default during the entire lifecycle of the development of the new large-scale IT systems.

Data protection impact assessments should not only be seen as an obligation for data controllers where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, but also a decision made by eu-LISA to achieve the above-mentioned objectives. The Agency may well decide to carry out DPIAs as a way to generate knowledge and data protection culture, analyse or audit data processing activities, improve the global process management or control the level of risk accepted in each data processing activity in a systematic, methodical and documented way.

DPIAs shall be considered a 'live' document subject to regular review or re-assessment should the nature, scope, context or purpose of the processing change for any reason. Therefore, DPIAs will become a continuous practice in the activities of eu-LISA and therefore, it shall be adequately embedded in its processes.

In line with the EDPS guidance[1] and WP29/EDPB guidelines on DPIAs[2], DPO has been supporting eu-LISA staff and its contractors on carrying out DPIAs. In 2019, focus was given to the start of the Entry Exit System DPIA. The DPO has been directly supporting eu-LISA contractors to progress with this assignment. In 2019, the DPO also started to prepare a comprehensive template to elaborate the DPIA report.

[1] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies

[2] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

It is key that, when DPIAs are externally contracted, eu-LISA selects specialised stakeholders that demonstrate sufficient guarantees to conduct DPIAs, for instance, by means of certified data protection professionals with appropriate knowledge and expertise in this field.

3.5 Projects and change management process

2019 has been a crucial year for eu-LISA. Its new mandate for the development and operational management of large scale IT systems translates into a huge increase in the number of changes and projects. eu-LISA is dealing with ambitious and complex projects with a very strong component in data protection.

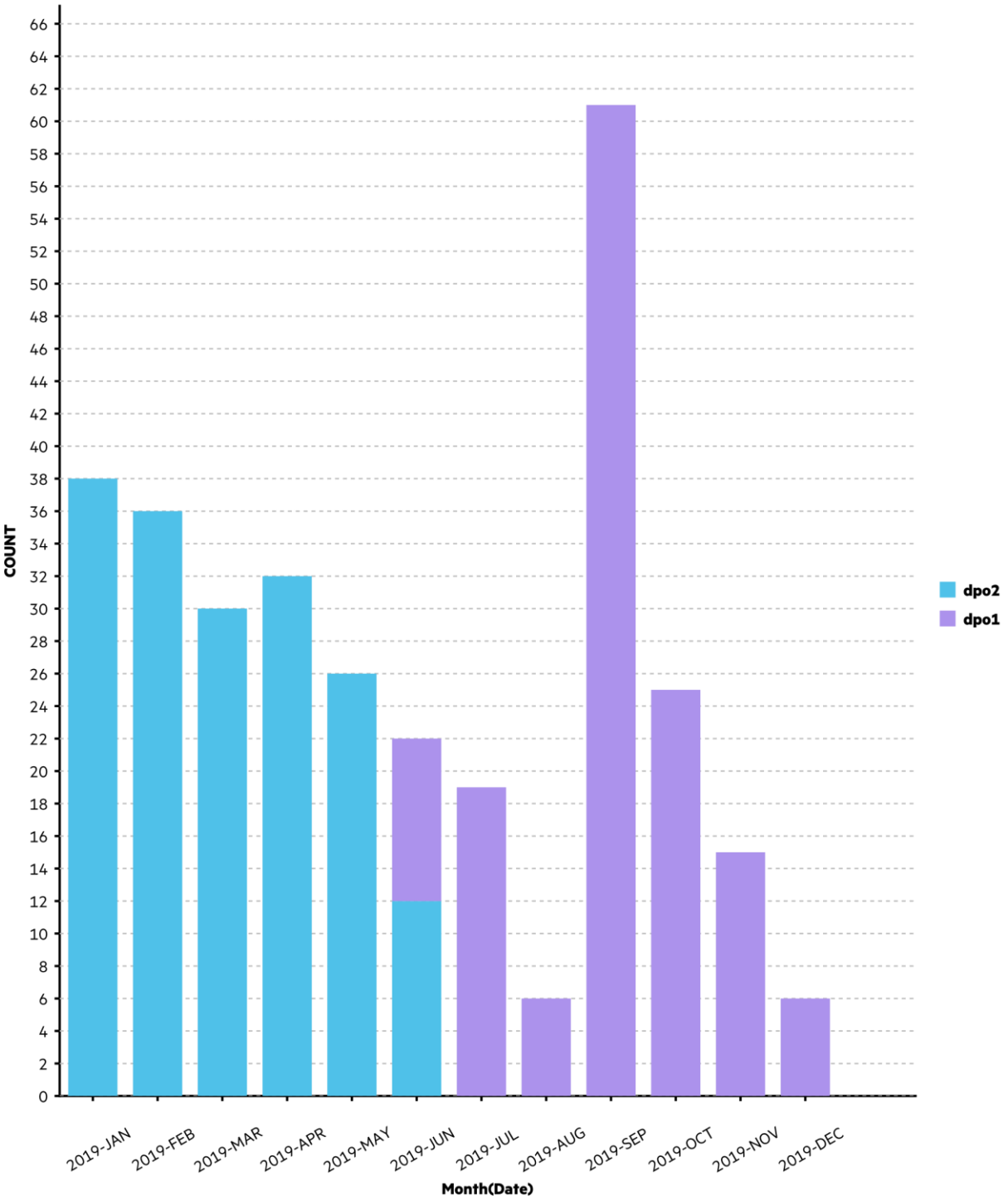
Therefore, the eu-LISA Project Management Methodology (PMM) shall integrate the appropriate checks and tools in regards to data protection. There are new data protection obligations that eu-LISA needs to comply with including data protection impact assessments. An effective PMM shall detect the data protection risks and requirements associated to every specific project at a very early stage. This will allow eu-LISA to plan the necessary resources, time and budget in every project.

eu-LISA shall ensure that the PMM does not overlook data protection risks and obligations, and shall take the necessary actions to align the PMM with the requirements of the new Regulation (EU) 2018/1725. The specific team in charge of the eu-LISA PMM shall benefit from the advice and guidance of the DPO to find out the best way to integrate them.

On the other hand, DPO is involved in the approval process of the Change Management procedure since the Management Board requested. Although this measure is very positive, the unbearable number of changes results in a disproportionate effort and makes this measure ineffective. Change Management procedure shall ensure that the data protection risks associated to any proposed changes are detected at an early stage. Therefore, the DPO strongly recommend that the Change Management procedure is revised with the view to introduce a new efficient and effective approach. This new approach should integrate checks and tool to detect, for instance, if the change is substantial enough to trigger the need to carry out a data protection impact assessment.

The owner of the Change Management procedure shall seek the advice of the DPO when addressing this task.

During 2019 the number of changes assigned to DPO role reached 316. The Acting DPO took care of these changes in the first half of the year and the new appointed DPO since June 2019. Details on the how changes were handled by month and by both DPOs are included in the chart below.



3.6 Procurement

The new data protection rules applied directly as from 11 December 2018. In order to ensure that contracts signed between eu-LISA (controller) and external companies (processors) are in line with Regulation (EU) 2018/1725, in particular Article 29, eu-LISA is including the new data protection clauses in the new contracts. For ongoing contracts, a risk assessment in relation to the subject matter of the contract was carried out, i.e. if personal data were to be processed or not by the contractor and if this is the core subject of the contract or not. Following this assessment, when justified by the subject matter of the contract in question, the contract will be amended in line with the new data

protection provisions.

3.7 Prior consultation on decisions and policies/procedures

The DPO is frequently consulted on the policies and procedures that might have an impact on the processing of personal data at eu-LISA.

3.8 Supervision and Collaboration

3.8.1 EDPS inspection and recommendations

In November 2018, the EDPS conducted an audit for the Schengen Information Systems (SIS II) and for the Visa Information System (VIS) in accordance with relevant international auditing standards. The purpose of the EDPS inspection was to check that the personal data processing activities of eu-LISA, as the Management Authority for both systems, are in accordance with the applicable data protection regulation. The audit went smoothly in the tone of good cooperation with the auditing authority. The EDPS draft report was received by eu-LISA in Q4 2019 and a consultation to the Management Board followed. Comments on the EDPS draft report will be formally adopted by eu-LISA Management Board in accordance with Article 19(1)(hh) of eu-LISA Regulation.

The DPO also acted as the liaison between eu-LISA and the EDPS for the inspection on the Eurodac system during Q3 and Q4 of 2019. The DPO provided an update of the status of the EDPS recommendations from the previous Eurodac inspection conducted in 2016. The DPO also collected all documentation requested by EDPS, prior and during the inspection. The audit on Eurodac was carried out at the beginning of December 2019.

The scope of the audit included a follow-up on the EDPS recommendations of the previous audit report, security and operational management of the Eurodac system, and the retention period of records and log files.

The EDPS also made an inquiry on the use of Microsoft products and services by EU institutions. It was launched in April. eu-LISA contributed by providing all information requested by EDPS.

During 2019, EDPS also started to proactively supervise the progress of the development of the European Travel Information and Authorisation System (ETIAS). Right after the closure of the Eurodac inspection carried out in the operational site of eu-LISA, eu-LISA DPO was requested to participate in a joint meeting with EDPS and the European Border and Coast Guard Agency (EBCG). The scope of the supervision on ETIAS was mainly focus on the integration of data protection aspects in the procurement process of ETIAS and how the data protection requirements are taken into account in the ETIAS technical specifications.

3.8.2 Supervision Coordination Groups for Eurodac, SIS II and VIS

Following the legal requirement of Article 5(1)(f) of the eu-LISA DPO Implementing Rules, by invitation of the Supervision Coordination Group (SCG) of Eurodac, SIS II and VIS, the DPO represented eu-LISA at these 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.

SCGs were informed about the latest developments and issues of the systems that may impact the processing of personal data. The SCG members were interested in how the systems were performing, in the related incidents, in the roll-out status of VIS and in the quality of the data. In addition, the DPO was requested to present current developments in relation to the European Travel Information and Authorization System (ETIAS) and the Entry/Exit system (EES). The SCG meetings were held in June and November 2019.

The DPO would like to remark the excellent collaboration and support from the Acting DPO and the colleagues from the eu-LISA Operational Department in Strasbourg.

3.8.3 JHAAs DPOs Network

In 2019, the Europol's DPO organised two meetings in The Hague. The newly appointed DPO attended both meetings.

In July, topics discussed included the new implementing rules for data protection officers, interoperability of the large scale IT systems, chapter IX of the Regulation (EU) 2018/1725 and new mandate of the EBCG. In September, eu-LISA new mandate was introduced and international transfers of personal data were part of the topics under discussion.

3.9 DPO Network meeting

In May 2019, the Acting DPO took part in the 45th DPO Network meeting hosted by the European Insurance and Occupational Pensions Authority (EIOPA) in Frankfurt. In November 2019, the newly appointed DPO attended the 46th DPO Network meeting held in the Historical Archives of the European Union in Florence. Several cases were studied including contracts with IT providers or archives, and other important topics such as data protection requirements in procurement processes were also discussed.

3.10 Annual Survey

Although this activity was part of the eu-LISA Programming Document 2019, the use of available resources have been allocated to provide data protection guidance and support to the Agency in regards to its highest priorities, mainly, the new and existing large-scale IT systems. Therefore, this activity was put on hold.

4 Data Protection Function

Article 44 of the Regulation (EU) 2018/1725 and Article 6 of the eu-LISA DPO Implementing Rules address the need to provide the DPO with the necessary resources to carry out his or her tasks and duties.

In this sense, a selection procedure was opened to select a Data Protection Assistant during the second half of 2019. The selected candidate, based in Strasbourg operational site, joined eu-LISA at the end of 2019. This position does not correspond with the Assistant DPO role foreseen in Article 3 of the eu-LISA DPO Implementing Rules.