PUBLIC

From: Encarna Gimenez, Data Protection Officer (DPO)

To: eu-LISA Management Board

Subject DPO Annual Work Report - 2020

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Vesilennuki 5 • 10415 Tallinn • Estonia

PUBLIC

DPO Annual Work Report - 2020

Data Protection Officer

Table of Contents

Document Control Information

Settings	Value
Document Title:	DPO Annual Work Report 2020
Document Author:	DPO
Revision Status:	Final
Issue Date:	01/March/2021

Summary of Changes:

Revision	Date	Created by	Short Description of Changes
[1]	*06/01/2021*	Intern to DPO	Initial draft
[2]	19/01/2021	DPO	Initial review
[3]	20/01/2021	Intern to DPO	Implementation of changes proposed by DPO
[4]	01/03/2021	DPO	Final version

1 Introduction

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 EU Large-Scale IT System.

eu-LISA Data Protection Officer (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).

Since the beginning of 2020, the COVID-19 pandemic has affected daily life of individuals and the work of all EU Institutions and bodies (EUI). In order to prevent and control the spread of this contagious disease among its staff and ensure business continuity, eu-LISA has adopted exceptional measures including a special teleworking regime. The use of new and enhanced IT solutions has grown exponentially. Other COVID-19 related measures have been introduced in the working space.

As a result, the processing of personal data - not only by eu-LISA but for all EUIs - have been seriously impacted. Common challenges and issues of concern were discussed, on one side, with the rest of DPOs from JHA agencies (JHAA) resulting in a Joint Statement on the topic, and on the other hand, within the network of DPOs from all EUIs.

The DPO of eu-LISA worked closely with the data controllers and EDPS to find both effective and compliant solutions that ensure the respect for privacy and personal data.

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 2020.

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 2020, the DPO of eu-LISA organised an awareness session in order 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 the Data Protection Officer and the European Data Protection Supervisor. More than 100 participants attended this interactive session.

In October 2020, an Awareness Session for newcomers was held with the aim of offering an overall approach to the basic concepts and principles of data protection and Regulation (EU) 2018/1725. Although eu-LISA newcomers was mainly the targeted audience of this training, the session was also open to the rest of eu-LISA personnel. Attendance reached 31 participants and their feedback showed that most of them liked the content and the presentation in itself.

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 on a regular basis including news items, templates and step-by-step instructions. In particular, a new section was created in the DPO intranet on 'Data Protection Impact Assessments' (DPIA) which explains in detail steps and actions to follow - when a DPIA is needed -.

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 (EU) 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. In addition, 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 2020, the **eu-LISA register of data processing activities** included **116 records**. Twelve of them were registered during 2020. The central register of processing operations is public, constantly updated and available from the eu-LISA website.

3.3 Personal Data Breaches

Following obligations stemming from article 34 (6) of the Regulation (EU) 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, four 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 controllers 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 (EU) 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 the 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 2020, focus was given to the start of the European Travel Information and Authorisation System[3] (ETIAS) DPIA, the start of the ECRIS-TCN[4] DPIA or the shared Biometric System[5] (sBMS) DPIA. The DPO has been directly supporting eu-LISA contractors to progress with these assignments. In 2020, the DPO made available a comprehensive template to elaborate the DPIA report and created a brand-new section on the DPO Intranet on DPIAs.

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 and extensive knowledge and expertise in this field.

At the end of February, the EDPS launched a survey for all EUIs focused on DPIAs. The DPO of eu-LISA contributed to this survey by providing her insights and the responses from eu-LISA to the EDPS questionnaire by beginning of April. This survey aimed to get a picture of the global state of play on EUI compliance with the data protection rules. EDPS wanted to lean on the practical approach, number of DPIAs conducted by EUIs or lessons learnt up to that date.

3.5 Change management process

DPO of eu-LISA 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 or to revisit an existing data protection impact assessment (DPIA).

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

During 2020, the number of changes assigned to DPO role reached 456, including changes not only for the development and operational management of the EU Large-Scale IT Systems but also those changes related to the regular functioning and administration of eu-LISA. In 2020, there has been an increase of 44% compared to the requests for change (RfC) that the DPO dealt with during 2019. The DPO of eu-LISA took care of the majority of these changes supported by the DPO Assistant.

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

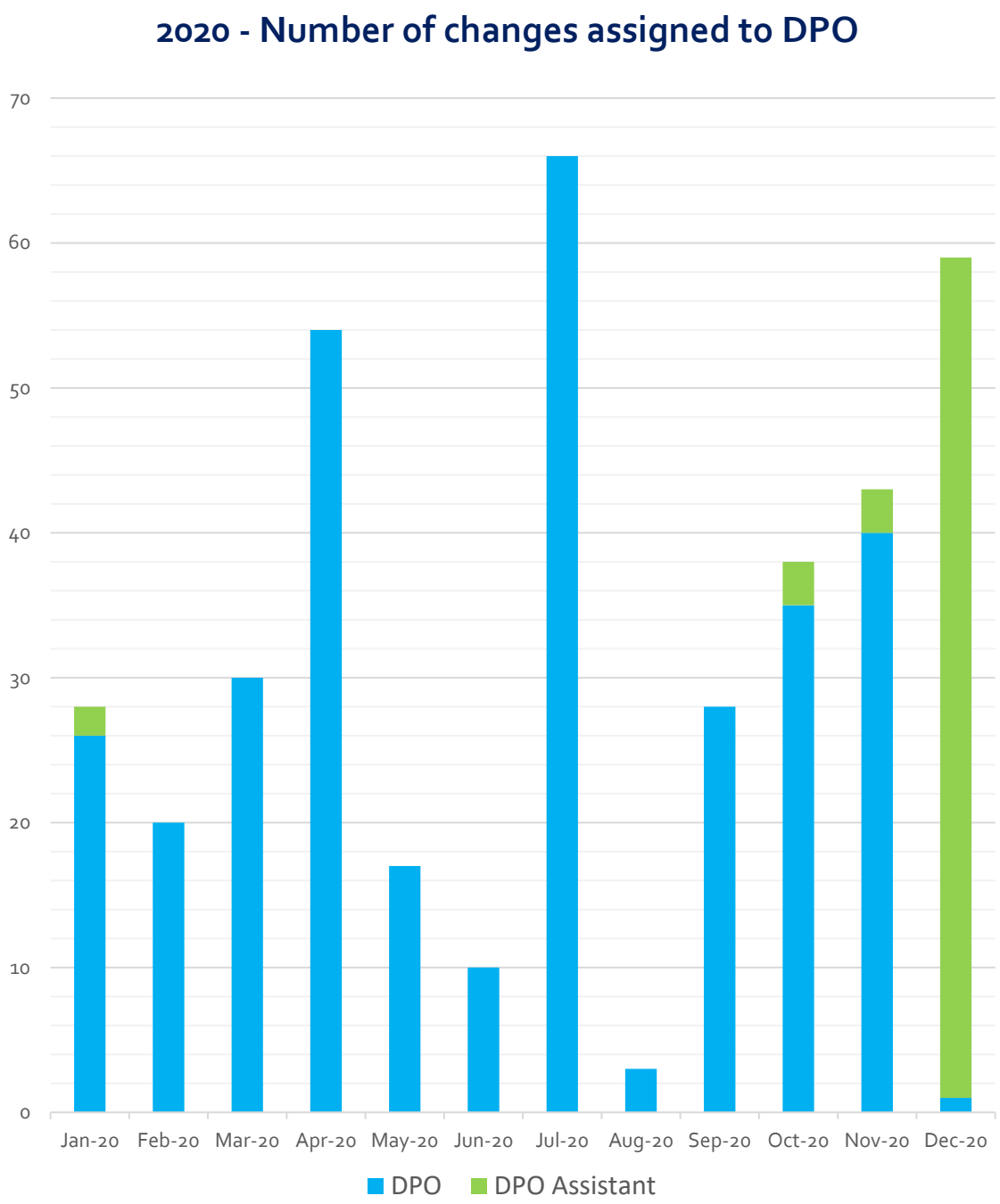
[2] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

[3] Regulation (EU) 2018/1240

[4] Regulation (EU) 2019/816

[5] Regulation (EU) 2019/817; Regulation (EU) 2019/818

Details on the how changes were handled by each of them per month are included in the chart below.



3.6 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.

In particular, in accordance with Article 15 of the eu-LISA DPO Implementing Rules, responsible staff shall seek the advice of the DPO when planning to apply restrictions on data subjects' rights. These rights should be strictly respected. Only under exceptional circumstances may be restricted and these restrictions shall be based on eu-LISA internal rules under Article 25(1) of Regulation (EU) 2018/1725.

Following the EDPS guidance from June 2020[6], the DPO of eu-LISA drafted internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of the functioning of eu-LISA. After consultation with eu-LISA Staff Committee and the EDPS, these internal rules will be submitted to the Management Board of eu-LISA for formal adoption.

3.7 Supervision and Collaboration

3.7.1 Virtual encounter between EDPS and eu-LISA

On 15 April 2020, the newly appointed European Data Protection Supervisor, Wojciech Rafal Wiewiórowski, and members of his team joined on a virtual meeting with eu-LISA's representatives and its DPO. The EDPS' visit to eu-LISA premises in Strasbourg planned for March 2020 had to be cancelled due the COVID-19 outbreak in Europe and resulting travel restrictions. This new fresh initiative supported both organisations' willingness to keep working together on the development and operational management of the EU Large-Scale IT Systems. The meeting, held via videoconference, was the first bilateral encounter between eu-LISA´s Executive Director and the EDPS. The virtual visit spanned over a couple of hours and included presentations and exchanges of views on several topics relevant to the EU Large-Scale IT Systems, including state of play of the existing ones, implementation of the new systems, or biometric accuracy and its effects on privacy and fundamental rights.

Both parties – the EDPS and the Executive Director of eu-LISA - expressed their openness to an active cooperation throughout the significant new extended mandate of eu-LISA.

3.7.2 EDPS inspections and recommendations

Ensuring a high level of data protection is one of the main objectives of the Agency. External audits on data protection compliance contribute to facilitate this goal and add value to the Agency's activities. Including audit recommendations as part of the eu-LISA continuous improvement plan for the operational management of the EU Large-Scale IT Systems makes this process much more effective.

3.7.2.1 SIS and VIS

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.

[6] Guidance on Article 25 of the Regulation (EU) 2018/1725 and internal rules restricting data subjects rights

The final EDPS report was received in April 2020 and contained 43 recommendations. eu-LISA has transposed all EDPS recommendations into an Action Plan. The DPO monitors the progress of its implementation and, to this extend, organises quarterly follow-ups with responsible staff. The follow-up on recommendations with deadline Q1-2020 took place during May 2020. Follow-up on recommendations with deadline Q2-2020 was conducted in July 2020, and in October 2020 for those recommendations with deadline Q3-2020. It is foreseen that recommendations having Q4-2020 as a deadline will be reviewed in January 2021. On behalf of eu-LISA, the DPO liaises with EDPS every quarter to proactively update on the progress and status of the recommendations.

3.7.2.2 Eurodac

At the beginning of December 2019, EDPS carried out and inspection on Eurodac system. The Draft EDPS Report on this inspection was received on 18 November 2020. In accordance with Article 19(1) (hh) of eu-LISA´s Establishing Regulation (EU) 2018/1726, the Management Board of eu-LISA shall adopt formal comments on this audit report before its final version is sent to the European Parliament, the Council, the Commission, the Agency, and the national supervisory authorities - following Article 31(2) of the Eurodac Regulation (EU) 603/2013.

For this purpose, the DPO of eu-LISA conducted an exercise to collect relevant feedback. This exercise included :

- an internal review in November 2020;
- a consultation with the Eurodac Advisory Group between 30 November and 14 December 2020; and
- a consultation with the Management Board from 22 December 2020 until 11 January.

All inputs were consolidated and a written procedure was launched on the 12 of January 2021 for a decision of the eu-LISA Management Board to adopt formal comments on the European Data Protection Supervisor (EDPS) inspection report with regard to Eurodac. On 18 January 2021, the written procedure was completed with no objections by the Board members with the right to vote and the formal comments were sent within the deadline set by EDPS.

3.7.2.3 Public register of data processing activities

At the beginning of 2020, the EDPS decided to screen how European Union Institutions and Bodies (EUIs) comply with the obligation to keep a publicly accessible central register. The first phase of this monitoring exercise was conducted remotely and unannounced to simulate availability to the public. At the end of the second phase of the inspection (11 March 2020), only 15 out of a total of 67 EUIs examined were considered fully compliant (according to the limited scope of the inspection). It should be noted, that eu-LISA was included in this group of compliant EUIs and has been listed within the best practice examples. At the end of May, the DPO enhanced the format of the Public Register to include further information and ensure a high level of transparency of the processing of personal data by eu-LISA.

3.7.2.4 EDPS order on International Data Transfers

In October 2020, all EUIs received an order from EDPS to conduct a mapping exercise of international data transfers to third countries and to report any identified risks and gaps based on the aforementioned exercise. Following this order, the DPO provided to eu-LISA's controllers meaningful assistance by sharing a template in the DPO intranet with the aim to map data transfers and by organising several meetings in order to address any queries concerning this exercise.

In this regard, DPO worked on a detailed report in order to identify the potential risks and gaps resulting from the reported international transfers. This report will help eu-LISA to carry out, in a second phase, a case by-case "transfer impact assessments" ('TIA') with the aim to identify whether an essentially equivalent level of protection as provided in the EU/EEA is afforded in the third country of destination. Concluding this second phase, eu-LISA should reach a decision of whether to continue or stop the international personal data transfers identified in the mapping exercise.

3.7.2.5 EDPS Survey on processing activities in Covid-19 times

In order to understand more of the reality on the EUIs during COVID-19 outbreak, EDPS decided to conduct a survey for all EUIs on this matter. The overall objective of this survey was to understand how EUIs comply with data protection requirements under Article 8 of the Charter of Fundamental Rights and Regulation (EU) 2018/1725.

For eu-LISA, the survey mainly focused on:

- New processing operations implemented by eu-LISA as part of their return to work strategy; and
- IT tools or solutions implemented or enhanced by eu-LISA to ensure business continuity in times of telework.

In this regard, the DPO prepared an initial inventory of data processing operations and IT tools that may be part of this survey in the areas of Security Unit, Human Resources Unit, Corporate Service Unit or Corporate Governance Department. The survey was launched on 18 December 2020 and the final deadline to report to EDPS was set to 31 March 2021.

3.7.3 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 EU Large-Scale IT Systems on operational matters.

During the meetings that were held in June and November 2020, the members of the 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, related incidents, rollout status of VIS and 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 DPO also presented the impact of Brexit in relation to United Kingdom records in Eurodac and the disconnection strategy from SIS.

Colleagues from different areas of eu-LISA are key to provide the most accurate information. Therefore, the DPO would like to remark the excellent collaboration and support from all of them.

3.8 JHAAs DPOs Network

The DPOs of eu-LISA attended the three online meetings of the DPOs of the JHA agencies (2 July, 29-30 September and 7 December 2020) that were organised by the DPO of Eurojust in 2020.

During these meetings, topics under discussions included the rules in application of Article 25 of Regulation (EU) 2018/1725, the new legal framework applicable at Eurojust since 12 December 2019 or the experiences regarding data breaches as well as with cooperation with the EDPS. Particular attention was given to the issue of international transfers, especially after the Schrems II judgement, and ideas were exchanged on how to deal with the subsequent EDPS order to all EUIs.

COVID-19 and related issues link to this pandemic were also lengthy discussed. The DPOs reflected on points of concern and shared experiences regarding the difficulties of operating under time pressure and the need to have clear and timely guidance from the EDPS, while at the same time having to consider the guidance given by the national Data Protection Authorities of the countries where the agencies have their seat.

These discussions led to the drafting of the *Joint Statement on issues related to the present COVID-19 pandemic*, annexed to this report. The joint statement was presented to the network of the DPOs of the EUIs on 10 December 2020. As a result, many DPOs of the EU institutions, agencies and bodies[7] endorsed the Statement.

3.9 DPO Network meeting

In May 2020, the DPO took part in the 47th DPO Network meeting hosted online for the first time due to COVID-19 outbreak. It covered various topics under the data protection domain were covered including the use of social media by EUIs – as means of communication and source of information -, registers of processing activities – best practices identified during EDPS inspection -, EDPS findings and recommendations on the use of Microsoft products and services as well as COVID-19 and data protection – the EU context, challenges, new trends in EUIs and tips to have in mind -.

7 EUROFOUND, REA, ECHA, ENISA, CEDEFOP, EFCA, EACEA, EUIPO and CPVO, CdT, ERC, EMA, EMSA, Council of the EU, Ombudsman, EFSA, EDA, EASME, European Parliament, EEAS, EU-OSHA and ECA

On 10-1 December 2020, the DPO virtually attended the 48th meeting of the Network of DPOs. The meeting covered various topics on data protection, in particular the strategy to comply with the Schrems II case, including supplementary measures or difficulties for controllers on this matter.

3.10 Annual Survey

Although this activity was part of the eu-LISA Programming Document 2020, the use of available resources has been allocated to provide data protection guidance and support to the Agency in regards to its highest priorities, mainly, the new and existing EU 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 process to select an additional Data Protection Assistant was opened during the second half of 2020. This second Data Protection Assistant will be based in Strasbourg operational site and (s)he is expected to join the team in Q2 2021.

5 Annex: Joint Statement of DPOs

JOINT STATEMENT OF DATA PROTECTION OFFICERS OF EUROPEAN UNION INSTITUTIONS, BODIES, AGENCIES AND OFFICES

8 January 2021

Since the beginning of 2020 the COVID-19 pandemic has affected in an unprecedented manner the life of all of us and continues affecting all organisations of the EU. It has raised many novel and complex issues which impact on the respect for privacy and the protection of personal data. Such issues touch upon managing the pandemic itself, which involves processing special categories of data concerning health in the context of activities such as temperature checks or contact tracing. The pandemic has also led to the development, or further strengthening, of teleworking and online working methods, which requires the selection or implementation of software for secure tele- and videoconferencing under exceptional time pressure.

The pandemic has shown the need for data controllers and senior management of EU organisations to consult DPOs at the earliest possible time and actively involve them in considering the issues at hand, which often require an urgent response. DPOs of EU organisations play a major role in assessing the compliance of considered processing with data protection principles, especially proportionality and necessity. The additional efforts required from DPOs in terms of resources and time investment in working on all these complex new issues should however not be underestimated.

The pandemic has also shown the need for the EDPS to strongly support and provide guidance to the DPOs when taking positions on these sensitive issues. In this context, the timely and specific guidance of the EDPS becomes of crucial importance for a coordinated and efficient management of the pandemic by organisations of the EU.

We as DPOs believe that efficiently managing the pandemic and complying with the data protection requirements, ensuring the respect for private life and the protection of personal data, is the only correct answer in these challenging times. We look forward to continuing working together with data controllers, senior management and the EDPS to find both efficient and compliant solutions to the novel issues raised by the pandemic.

This statement was issued on 7 December 2020 by the DPOs of the JHA agencies : Diana Alonso Blas, DPO Eurojust (chair), Daniel Drewer, DP Function, Europol; Encarna Gimenez, eu-LISA DPO; Alexandru George Grigore, EASO DPO; Olli Kalha, DPO CEPOL; Nayra Perez, DPO Frontex; Robert Jan Uhl, DPO FRA; Ieva Vasiliune, DPO EIGE; Ignacio Vázquez Moliní, EMCDDA DPO.

After its presentation at the meeting of the EU DPOs on 10 December 2020, the statement has been endorsed by: Mafalda Aguilar, EUROFOUND; Bo Balduyck, ECHA; Athena Bourka, ENISA; Jesus Bustamante, CEDEFOF; Stefano Donadello, EFSA; Radostina Nedeva-Magerlein, EMSA; Reyes Otero Zapata, Council of the EU; Francesca Pavesi, Ombudsman; Claus Reunis, EFSA; Clarisse Ribeiro, EDA; Elke Riviere, EASME; Secondo Sabbioni, European Parliament; Emese Savoia-Keleti, EEAS; Michaela Seifert, EU-OSHA; Marino Stefano, EMA; Johan Van Damme, ECA.