EUROPOL

Annual Report of the Data Protection Officer 2021

EDOC#1196888

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AP	Analysis Project
AI	Artificial Intelligence
CAB	Corporate Affairs Bureau
CCTV	Closed-Circuit Television
CFN	Computer Forensic Network
CPDP	Computer, Privacy and Data Protection
CtW	Check the Web
DEDC	Deputy Executive Director Capabilities
DEDG	Deputy Executive Director Governance
DG FISMA	Directorate General for Financial Stability, Financial Services and Capital Markets Union
DPCP	Data Protection Contact Point
DPF	Data Protection Function
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECB	Europol Cooperation Board
EC3	European Cybercrime Centre
ECRIS-TCN	European Criminal Records Information System for Third-Country Nationals
ECTC	European Counter Terrorism Centre
ECJ	European Court of Justice
EDPC	Europol Data Protection Champion
EDEN	Europol Data Protection Experts Network
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EFECC	European Financial and Economic Crime Centre
EIPA	European Institute of Public Administration
EMSC	European Migrant Smuggling Centre
ENU	Europol National Unit
EPE	Europol Platform for Experts
ER	Europol Regulation
ERA	Academy of European Law
ESOCC	European Serious and Organised Crime Centre
ETIAS	EU Travel Information and Authorisation System
EU	European Union

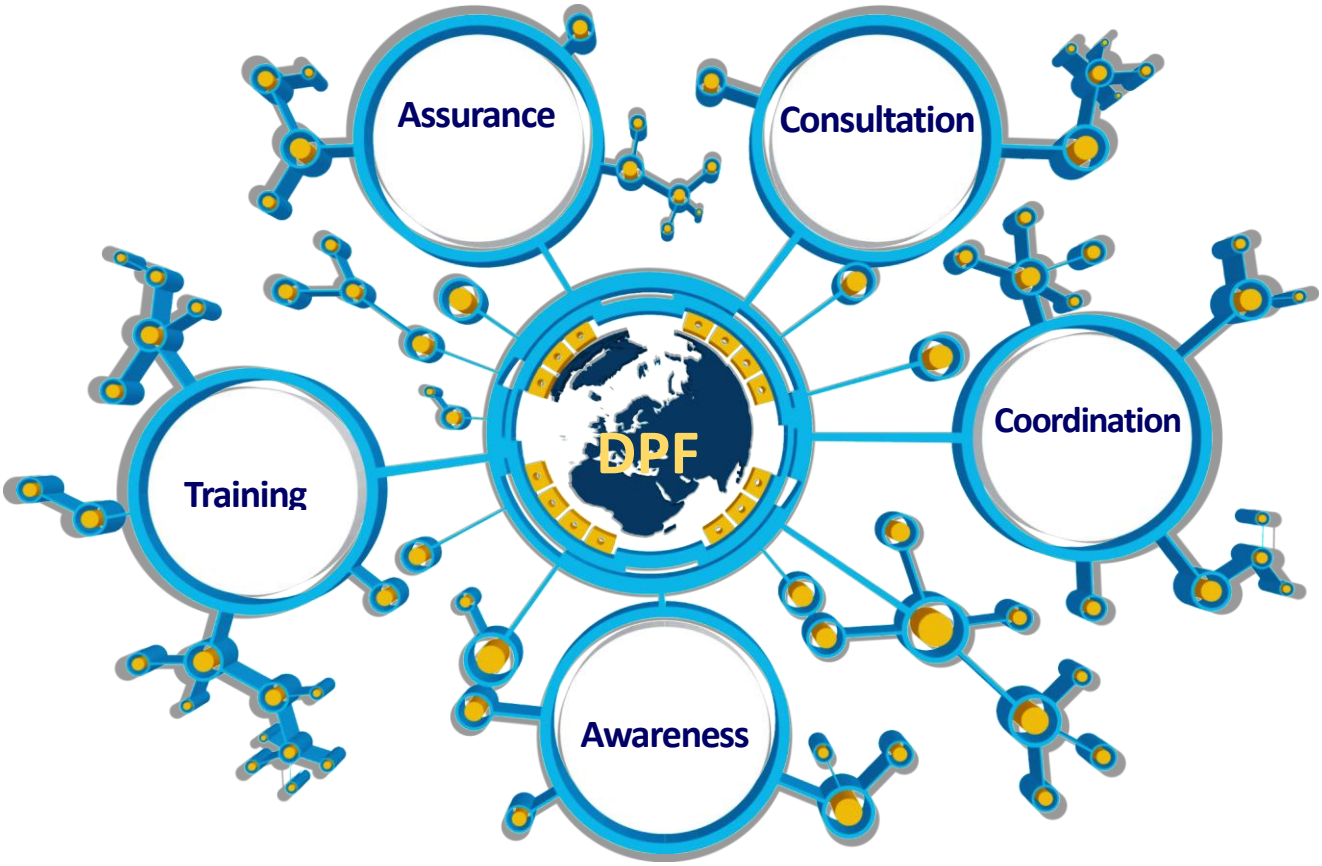
EUDPR	Regulation on the protection of personal data by EU agencies
EU IRU	EU Internet Referral Unit
EURODAC	European Dactyloscopy database
FITE	Forensic IT Environment
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
GRACE	Global Response Against Child Exploitation
GO	Guest Officer
H4U	Here For You
HENU	Head of Europol National Unit
HOS	Horizontal Operational Services
JHA	Justice and Home Affairs
JPSG	Joint Parliamentary Scrutiny Group
LE	Law Enforcement
MB	Management Board
MB WG CM	Management Board Working Group on Corporate Matters
MB WG IM	Management Board Working Group on Information Management
MEP	Member of the European Parliament
NGO	Non-Governmental Organisation
OAC	Operational and Analysis Centre
OCG	Organised Crime Group
OSP	Online Service Provider
OTF	Operational Task Force
PIU	Passenger Information Unit
PNR	Passenger Name Record
SIENA	Secure Information Exchange Network Application
SIP	Session Initiation Protocol
SIS	Schengen Information System
TFTP	Terrorist Finance Tracking Programme
TI	Travel Intelligence
UAS	Unified Audit Solution
UN	United Nations
US	United States
US DoT	US Department of Treasury
VC	Videoconference
VIDTF	Victim Identification Taskforce
VIS	VISA Information System

1. OVERVIEW

The Europol Regulation[1] (ER) foresees the preparation of an annual report, and the communication of this report to the Management Board (MB) and the European Data Protection Supervisor (EDPS), to be one of the main tasks of the Data Protection Officer (DPO).

The DPO and Head of the Data Protection Function (DPF) is accountable to the MB. He has to ensure, in an independent manner, that the processing of personal data by Europol, including personal data relating to staff members, is done in a way that is in compliance with the provisions set out in the ER. According to his mission the DPO provides objective assurance and consultation, which is designed to add value to and improve Europol's data processing operations. In the performance of his duties the DPO is supported by the colleagues in the DPF.

As previous annual reports, it covers the main assurance, consultation, coordination, training and awareness activities undertaken by the DPF. The main focus is on activities related to the statutory tasks of the DPO referred to in Article 41 ER, the Decision of the MB laying down implementing Rules concerning the DPO (#845687) and Article 45 Regulation 2018/1725 (EUDPR)[2].



[1] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)

[2] 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

This annual report covers 2021 as the second year in a row that was also determined by the impact of the pandemic on the work of Europol including the activities of the DPF.

The DPF monitored, informed and advised the agency about the related rules on the processing of health data and any new guidance for the processing of personal data in this pandemic context.

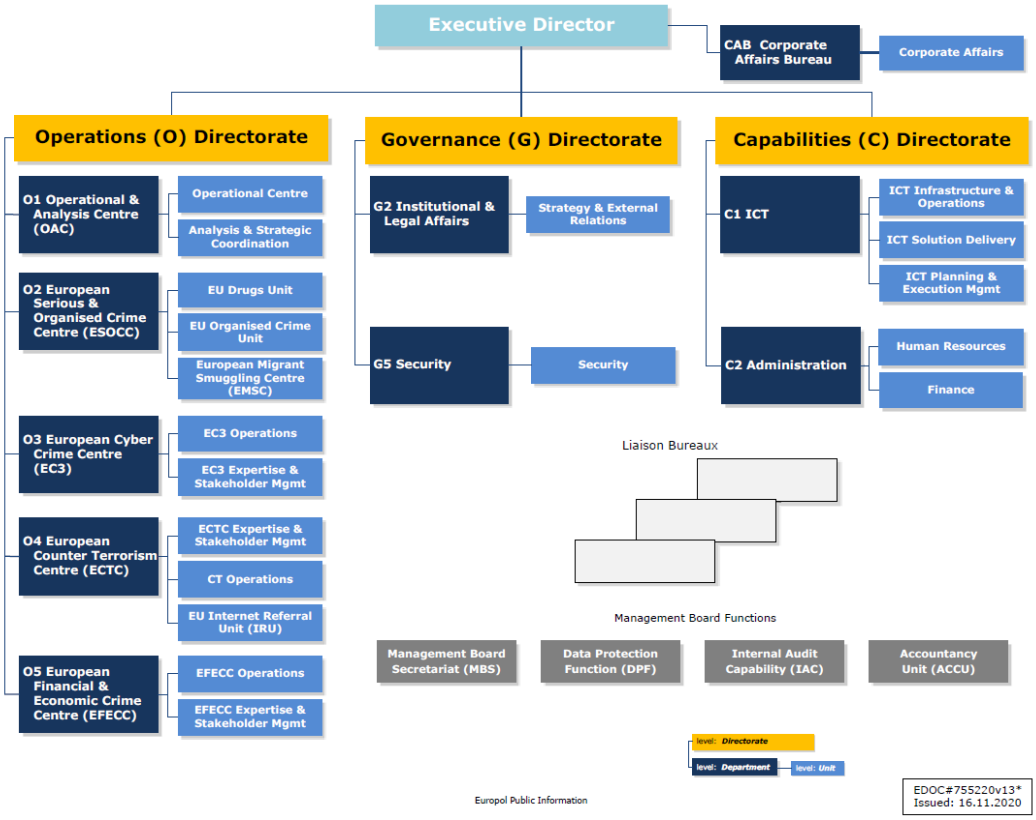
The EDPS highlighted in its communication to all agencies and bodies of the EU that the pandemic brings a higher risks in relation to the occurrence of data breaches.

Also 2021 saw a steadily growing demand from the controllers to the DPF for guidance and support in all areas of Europol's data processing activities. This was accompanied by enhanced demands of Europol's supervisory authorities, EDPS and ECB, towards the agency and the growing complexity of Europol's legal framework for the processing of personal data. The DPO and his staff continued to fulfil in 2021 all statutory duties, but due to staff shortages the DPF had to reduce activities in particular in the area of training, coordination and awareness.

2. GENERAL MATTERS

2.1. Assurance Role of the Data Protection Officer

The DPO as second line assurance provider for data protection compliance is positioned in the organigram next to the other three MB Functions. The DPO embedment as MB Function also safeguards the requirement of independency as stipulated in Article 41 (1) ER ("In the performance of his or her duties, he or she shall act independently").



Europol's tailor-made data protection framework is widely recognised as adhering to the highest standards of data protection in law enforcement. It is designed to serve the needs of the operational units in preventing and combating serious and organised crime and terrorism, while at the same time protecting the personal data processed in Europol's systems. The protection of personal data remains one of the key factors which enables Europol to successfully fulfil its mission.

Article 41(1) ER provides for a mind-independent judgment of the DPO regarding data protection matters. His advice as assurance provider serves as guidance for decisions made by the controllers regarding the implementation of effective and appropriate data protection safeguards.

The capabilities of the DPO are shaped by his right to access all data processed by Europol and all Europol premises. An escalation procedure as *ultima ratio* in case his advice would be ignored, which involves the Executive Director (ED) of Europol, the MB and the EDPS, lends power to this model of functional independence.

A related process description[3] contemplates the insertion of DPO recommendations into the corporate risk log which is, together with the regular communication to the ED and other controllers, a formal step prior to an escalation procedure. Due to constant communication with all stakeholders on matters of data protection compliance the DPO fulfilled his assurance role in 2021 without the need to initiate a formal escalation procedure according to Art. 41 (9) ER.

In addition, there is the possibility for the MB, the ED, any controller or data subject working at Europol to consult the DPO with regard to the interpretation or application of the ER and its implementing rules[4].

The DPO also has the possibility to perform inquiries into matters and occurrences directly related to his tasks. This can be done at own initiative or on request of the MB, the ED, the controllers and the data subjects working at Europol.

Finally, the accountability principle is part of the DPO Implementing Rules. The accountability principle stipulates that it is the responsibility of the controllers as first line assurance provider and in charge of the controls to ensure that all processing operations involving personal data within their area(s) of responsibility comply with the ER and EUDPR.

The functional role of the DPO of Europol as assurance provider is almost identical to the role of DPO in all other European Union (EU) agencies and institutions. However, the criticality of processing operations for law enforcement purposes at Europol, the applicability of two different legal regimes, the amount of personal data processed and the importance of data protection compliance for Europol's core business makes the portfolio of the Europol DPO distinct from the portfolio of other Data Protection Officers.

In addition to law enforcement data, the DPO also ensures the protection of Europol staff data since 11 December 2018 determined by Regulation (EU) No 2018/1725.

Compliance with this framework is not only a legal obligation for all EU bodies and agencies, but is also recognised by Europol's management as serving the interests of both the agency and its staff members.

[3] EDOC #977385v3

[4] Article 6(15) DPO Implementing Rules

2.2. Data Protection Function Resources

At the beginning of 2021 seven posts were allocated to the DPF. The function consisted of a Head of MB Function, one Senior Specialist, three Specialists, one Contract Agent Lawyer and one Contract Agent Office Assistant.

Due to the impact of the pandemic also in 2021 DPF colleagues switched to teleworking whenever instructed to do so by the Crisis Management Team (CMT) of Europol. Remote DPF access to both, CorpNet and OpsNet for data protection compliance purposes was arranged. The Head of the DPF ensured his presence at the headquarters to largest extent.

Throughout 2021 the DPF had to cope with a shortage of staff. One DPF specialist was on maternity leave from mid-July until the beginning of December. Furthermore, following the resignation of the Contract Agent Office Assistant in July 2021, the successor took up her duties in August 2021. As of September 2021 one of the Specialists was granted an internal transfer. The post has not been reallocated to the DPF yet.

Towards the end of 2021 the DPF could initiate a recruitment procedure for a Contract Agent with the specific task to assist the organisation to implement research and innovation projects in a data protection compliant manner. This post is a temporary reinforcement dependant on budget from H2020 projects envisaged for a maximum period of two years.

At the start of 2022 a reserve list was established for specialist post dedicated to operational data protection. It is foreseen that the DPF can recruit two specialists by the end of 2022.

The workload of the DPF remained on a very high level in 2021. As in the preceding year, this was partly due to the significant support required by the data controller regarding the proceedings related to prior consultation cases brought to the EDPS according to Article 39 ER. Furthermore, data protection advice regarding the establishment of the Europol Medical Service, the processing of personal data with regard to COVID-19 contributed to the increased workload together with the increase of data subject access requests resulting in 32 full hits dealt with by the DPF during 2021.

Also the overall increase of Europol's activities paired with an increase of operational personal data processed by Europol, the continued high number of recommendations provided by the EDPS in various business areas in the context of inspections, inquiries and prior consultations contributed to the increased workload of the DPF.

The DPF has always given priority to assuring internal compliance of Europol's operational core business within the applicable data protection framework and to provide for this purpose objective assurance and consultation activities designed to add value and improve Europol's operations.

2.3. Data Protection Awareness and Training

Article 41(6) (d) ER establishes that the DPO is tasked to cooperate "with Europol staff responsible for procedures, training and advice on data processing." However, the DPF has prepared and also delivered data protection briefings and awareness activities throughout 2021. Continued awareness raising engages staff members and enables them to understand how important data protection compliance is to maintain the trust of the data providers.

The DPF continued to foster data protection culture within the organisation by training staff members as well as external stakeholders. Due to the pandemic most trainings had to be provided in an online setting.

2.3.1. Newcomers Training

Prerequisite to the newcomers induction session on data protection is the e-learning module "Your data protection rescue guide" which summarises important information on data protection at Europol with the aim to raise awareness and improve knowledge on European data protection rules as well as Europol's data protection framework. It allows the target audience to learn about the fundamental rules for the protection of personal data, especially in the context of the EU and its institutions; to understand the specificity of data protection issues in the context of police and law-enforcement cooperation; to understand the role of the DPO and of the DPF at Europol; to acquire knowledge of rights and obligations in relation to personal data.

The monthly newcomer's induction session reinforced the knowledge acquired with the e-learning module by focusing on data protection principles and processing purposes, data subject access rights, prior consultations, personal data breaches, transfer of personal data to third countries and international organisations, data protection supervision and COVID-19. In 2021 the DPF provided the newcomers induction programme on data protection to in total 323 colleagues.

2.3.2. Guest Officer Training

In 2021 two Guest Officer trainings were provided. The aim of the training is to provide a comprehensive overview of the main issues at stake concerning the processing of operational personal data in the context of the migration crisis and the hotspots. It focuses on the applicable data protection regime and the specifics of hotspots data by emphasising human rights of asylum seekers and refugees as well as the specifics of the GO role in supporting national competent authorities. The training elaborates operational data processing activities in the hotspots including referrals, queries of Europol systems, relevant analysis projects and Art. 18(6) ER.

Worth noticing is that the DPF training was the only briefing that obtained 100% satisfaction on the satisfaction survey of the attendants in 2021.

2.3.3. Awareness trainings to extranl stakeholders

Together with the DPOs of Council and Eurojust as well as the EDPS, the DPO continued to provide lectures at the Data Protection Certification course organised by the European Institute of Public Administration (EIPA) in June and December 2021.

The Data Protection Certification course is dedicated to staff from the European Union Institutions, bodies and agencies.

The DPO also contributed to the Academy of European Law (ERA) seminar on Data Protection, the Law Enforcement Directive and European Criminal Justice in May 2021 in an online format.

2.3.4. Internal training on administrative data processing

On request of C2-01 Facilities, the DPF organised a specialised training for contractors dealing with administrative data processing with an accent on practical examples and

good practices in dealing with processing of administrative personal data. The training took place in July 2021.

2.4. European Data Protection Day

On 28 January 1981 the Council of Europe signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108. Marking the first legally binding international law regarding data protection, the Data Protection Day raises awareness for data protection and seeks to promote good data privacy practice across the EU.

In 2021 the Data Protection Day was celebrated with a clip distributed via social media channels featuring the Executive Director emphasising the importance of a positive data protection culture in order to be successful in the digital age – especially for law enforcement!

The Executive Director stressed that only if we preserve both - Freedom AND Security – the organisation will maintain the trust of citizens which is essential for police work. She encouraged the audience to join her in becoming a member of the Europol Data Protection Experts Network (EDEN) and to share ideas on how to get it right. The clip can be found online here: https://www.youtube.com/watch?v=ZN5IOPoxaDU

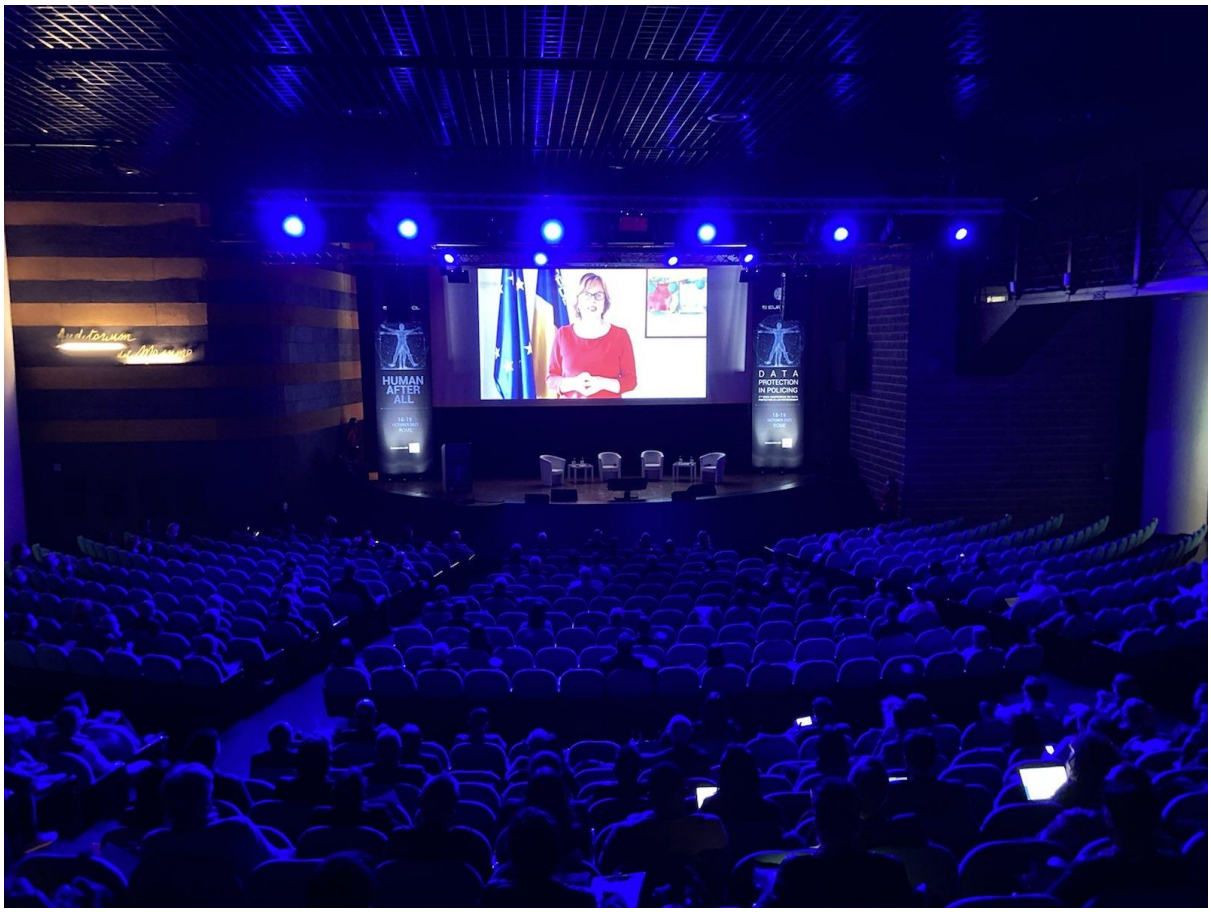
2.5. Europol Data Protection Experts Network

The **E**uropol **D**ata Protection **E**xperts **N**etwork (EDEN) within the Europol Platform for Experts (EPE) is an online collaboration platform which has been developed with the aim of involving stakeholders from various backgrounds including law enforcement as well as representatives of relevant private parties, academia and NGOs.

EDEN is used as a channel to present projects, best practices and events linked to data protection in a law enforcement context. It is an "on invitation only" network not suitable

for the exchange of operational personal data or classified information and has currently more than 600 active members.

The main focus throughout 2021 was to prepare the 7th EDEN event. Despite the COVID-19 restrictions and the challenges they impose on conference organisers, the 7th EDEN event took place face-to-face in Rome on 18/19 October. It was hosted by the Central Criminal Police Directorate of the Italian Ministry of Interior and co-hosted by the European Law Academy (ERA).



EDEN is all about the possibility of increasing security without unnecessarily decreasing citizen's freedoms. The link to security in everything Europol does is rather obvious. Engaging visuals and soundtracks were used throughout the event to potentiate the panel discussions and speakers' messages and visualise the organisation's commitment to freedom.

The concept of the conference was to bring together a very diverse group of representatives from different sectors, both on stage and within the audience, which usually speak a lot about each other – but hardly ever exchange views directly. Speakers were selected and invited based on their proven professional knowledge and expertise in the various subject matter areas. Particular focus was put on their ability to convey their respective message in an informative but also entertaining way.

The title of the 7th EDEN event "Human After All – Data Protection in Policing" reflected the importance of human factor in data protection which, under the light of the increasing use of Artificial Intelligence (AI) and Automated Data Processing, becomes more and more relevant. The human element remains steadily the building block of a

healthy data protection culture in any organisation, including in law enforcement agencies.

Related keynotes were delivered by Europol's Executive Director, Catherine De Bolle, the European Data Protection Supervisor, Wojciech Wiewiórowski as well as the Deputy Director-General of Public Security, Vittorio Rizzi, the Deputy Director-General for Security – DG HOME, Olivier Onidi, and the Director of the EU Agency for Fundamental Rights, Michael O'Flaherty.

The EDEN panels explored data protection issues related to facial recognition in policing, data literacy in law enforcement, the human intervention in AI, the risks of minors online as well as future trends and challenges in cybersecurity and data protection.

EDEN hosted in 2021 its own panel as part of the "Computer, Privacy and Data Protection (CPCP) Conference" for the second time. CPDP is the leading data protection and privacy conferences in Europe and around the world.

The topic chosen for the EDEN panel focused on online radicalisation in its various contexts including right-wing as well as Islamist extremism. The session reflected on the role of law enforcement and highlighted in how far data protection plays an important role being an asset in generating trust of citizens by determining what authorities can and cannot do when processing personal data in the performance of their duties.

2.6. Law Enforcement DPO Network

Since May 2018 the Police and Justice Data Protection Directive applies to both, cross-border and national processing of data by EU Member States' law enforcement and judicial authorities. One of the requirements is to appoint DPOs in national law enforcement authorities. The aim of the Law Enforcement DPO network hosted by Europol is that of sharing best practices, ideas and methods for state of the art data protection in the law enforcement sector.

In addition the Law Enforcement (LE) DPO Network provides national DPO colleagues a platform to cooperate. This is not only for the benefit of national law enforcement authorities when it comes to challenges regarding interoperability of the necessary cooperation regarding the response to data subject requests. It is also in the interest of Europol as it is going to facilitate operational business in full compliance with data protection requirements. Discussions in the LE DPO Network mirror the topics under scrutiny by the national Data Protection Authorities represented in the ECB. The same is valid for the scrutiny applied by the EDPS and national data protection supervisory authorities in the framework of joint inspections at Europol. The DPF plays a key role in the facilitation of communication on these cross-law enforcement agency topics.

This initiative can rely on Europol's financial support, with the approval of a budget line to fund travel expenses of one DPO of a national competent authority per EU Member State for two meetings per year of the EDEN LE DPO Network. Due to COVID-19 restrictions only one physical meeting was possible in 2021 held in the margins of the EDEN Conference in Rome, Italy, on 18/19 October. Topics discussed included DPO responsibilities in practice as assurance providers, data processor agreements in the area of law enforcement, third party cooperation and its practical challenges, usage of apps and services and modalities for cooperation with Facebook.

The second Law Enforcement DPO Network was held online on 16 December and included a presentation by CEPOL on their Fundamental Rights Training strategy with a view to assessing possibilities of a dedicated Law Enforcement DPO training to be provided as of 2023.

The Law Enforcement DPO Network no longer just provides the platform for the secure exchange between Law Enforcement DPOs. In 2021 and in response to respective requests, the platform has also been equipped with private sub-sites for various additional law enforcement related DPO groups within the EDEN community. A sub-site is a separate site that is connected to the platform to create different content that should be visible only for a subset of the audience of the parent platform. Sub-sites within a platform can also have different site managers. Currently, the following sub-sites have been created next to the EDEN Law Enforcement DPO Network:

- EDEN FIU DPO Network
- EDEN JHA DPO Network
- EDEN Justice DPO Network
- EDEN PIU DPO Network

2.7. Data Protection Function Internships

Already since 2010 the DPF is running regular internships which have produced tangible positive results for both Europol and the interns themselves. This was also the case in 2020.

Former DPF interns have evidently benefitted from the experience with many of them meanwhile pursuing impressive career paths in one or the other way linked to the projects they have completed at Europol. This includes employment in global law firms and consultancies as Data Protection and Privacy Specialists, a Policy Advisor to a MEP with specialist expert area in privacy and data protection, a Junior Risk and Compliance Manager Data Protection and Anti Money Laundering at a global company, legal researchers and many more. Also two DPF contract agents are in fact former interns of the DPF.

2.8. External Activities

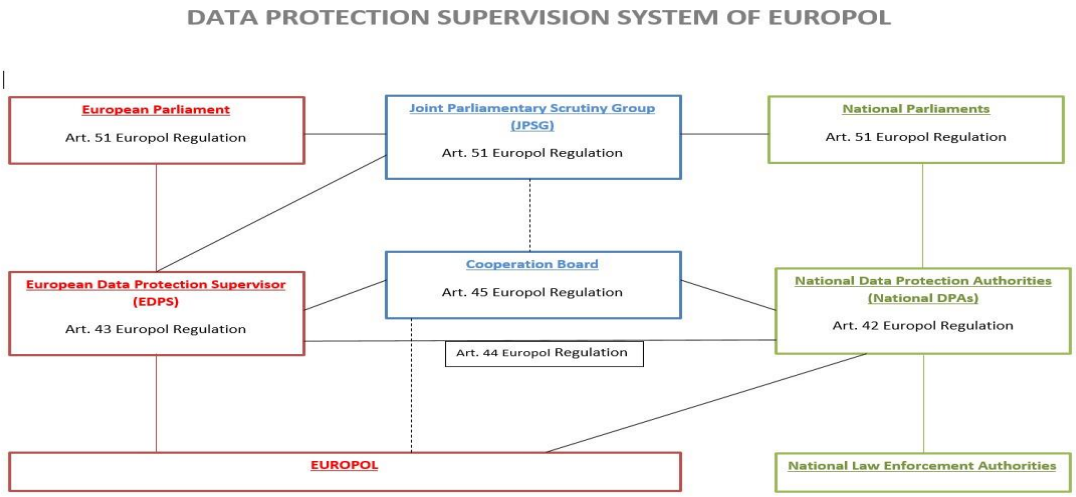
The DPF proactively exercised strategic leverage on important issues for the law enforcement community. In the operational domain the DPO continued the close cooperation with DPOs working for Justice and Home Affairs (JHA) agencies. DPF representatives attended several data protection sessions in which concrete links with Europol's operational business were identified.

DPF representatives have been requested to provide several keynote speeches in conferences and workshops. The DPO is prioritising and accepting participation only in the most relevant events from a law enforcement perspective, declining other less pertinent invitations.

2.9. Single Point of Contact for Data Protection Supervision

A core task of the DPO is to cooperate on behalf of the controllers with the data protection supervisory authority as well as the national data protection authorities.

This activity increased substantially with the data protection supervisory system under the Europol Regulation entailing cooperation with the EDPS as well as with national data protection authorities, the latter mainly via the ECB.



2.9.1. Regular Working Level Meetings

In 2021 the cooperation with the EDPS developed further even though, due to the pandemic, the same as last year, meetings mostly had to be carried out online.

Six regular working level meetings throughout 2021 addressed topics such as updates on Brexit and WA with UK, follow-up on FIU.net - legal basis for Europol storage of copy of UK database for the purpose of potential reconnection of UK to FIU.net, updates on Covid-19, follow-up EDPS inspection recommendations, Quest+, Hit/no hit system with Eurojust, Article 39 OSP and GRACE, NEO project update, Cross Domain Solution (CDS) DPIA, Machine Learning prior consultation opinion follow-up, SIS II fingerprint searches and other.

Furthermore, the DPF *facilitated* a high level meeting between the Executive Director of Europol and the EDPS early in December 2021 on the so called *Big Data Challenge*.

2.9.2. EDPS Inspections

The EDPS annual inspection carried out on 27/28 September focussed on the **development and use of artificial intelligence components for operational analysis** at Europol as well as the **data protection risk assessment (DPIA) process** in accordance with Article 39 ER.

By letter dated 19 July 2021 (EDOC#1179200), the *EDPS informed that he decided to target the following areas during the inspection:*

The development and use of machine learning models for the analysis of operational data collected in the context of specified OTFs.

The data protection risk assessment process leading to the decision to submit a prior consultation to the EDPS under Article 39 of the Europol Regulation.

The wording set out in the inspection mandate included an "Interview with Europol staff in EMMA and LIMIT responsible for the selection of training data and support to the team involved in the design and validation of the ML models. Checks on the systems to see the propagation of information from the output of the ML software to the further processing of that information in the operational systems."

Europol on 21 September once again confirmed to the EDPS that no such processing operations existed following the halt of all machine learning related processing

operations upon personal data, including the related development/training of machine learning tools, in view of the EDPS observations (C 2021-0130, letter of 5 March 2021, Section 3.1), as confirmed by the Deputy Executive Director Operations (EDOC-#1161545, letter of 4 April 2021, page 4). However, in the preparation of the inspection Europol then considered whether the use of operational personal data for the purpose of training the machine learning models could be reinitiated on the basis of the referred quote from the inspection mandate. The EDPS was consulted respectively.

By email dated 24 September the Supervisor stated that in light of the information provided by Europol in the context of the preparation of the inspection and of the follow-up of EDPS Opinion of 4 March 2021 (case file 2021-0130), the EDPS would like to take the opportunity of the inspection to get a better understanding of the procedures and safeguards put in place to minimise the data protection risks linked to the use of machine learning models, before agreeing to the processing of operational personal data in the context of OTF EMMA and LIMIT. This would allow the supervisory authority to make an informed decision, irrespective of the additional recommendations that can be included in the inspection report.

The inspection was carried out by ten EDPS inspectors in three thematic teams, i.e. one team dealing with the data protection risk assessment process, another team focussing on the development and testing of machine learning models and a third team focussing on operational data handling.

In their closing remarks, the EDPS inspection team members declared that they intend to progress the on-going prior consultation on the "Machine Learning Toolbox" *(Case 2021-0130)* as a matter of priority, taking advantage of inspection insights. The aim was to conclude the prior consultation as soon as possible and independent from the above outlined inspection timeline considering the operational urgency. The outcome of the prior consultation can be found below in the related dedicated chapter of this DPO Annual Report.

The supervisory authority complimented Europol on the organisation of the inspection and highlighted positively the very close cooperation between the operational colleagues and the DPF on the files inspected.

Europol received the draft minutes of the EDPS annual inspection on 28 October, comments were provided by 8 November 2021 in line with the stipulated EDPS deadline.

2.9.3. EDPS Inquiries

In the context of the on-going cooperation between Europol and the EDPS to ensure that the processing of personal data on persons under the age of 18 complies with the restrictions contained in Article 30 ER, and in light of the particular sensitivity that surrounds the processing of personal data of persons under 15 (given that the minimal age of criminal responsibility is defined as 14 or 15 in most Member States), Europol provided the EDPS with regular (annual or biannual) statistics on the processing of persons under 15 in the EAS.

On 07/10/20 the EDPS thus requested Europol to provide the current statistics on the processing of persons under 15 in the EAS including, in particular, the number of persons under 15, per year of birth (2005 and after), originator (source), Analysis Projects and personal implications. The EDPS informed Europol that they will get in touch with the competent supervisory authorities during the next meeting of the Europol Cooperation Board scheduled on 22/11/2020 of the amount of personal data transferred by each Member State to Europol in order to support their own supervisory activities on the processing of personal data on minors under the age of 15 at national level.

On the basis of this meeting, the DPF was approached either directly by the competent national authorities or via the EDPS to request more information concerning the minors (in particular SIENA numbers), allowing the information to be easily identified and further checked for its data protection compliance. The DPF provided support to the EDPS and to the national data protection supervisory authorities on four inquiries which took place in 2021 on the basis of Article 42 of the Europol Regulation.

2.9.4. Consultation of the EDPS

In 2021, the DPF consulted the EDPS in the process of modifications of the Manual for confidential counsellors and staff members on anti-harassment procedures to bring it in line with the EDPS recommendations. The consultation was inspired by a question raised by HR on whether **the decision to appoint a staff member as a confidential counsellor as a decision which is subject to Art. 90 (2) EUSR**.

2.9.5. Complaints towards the EDPS

There are three on-going complaint cases on the decisions taken by Europol with regard to data subject access requests under Article 36 Europol Regulation. It should be noted that only three complaint cases (on-going since previous years) compared to more than thousands of requests handled in the meantime demonstrates the implementation of a smooth administrative process together with high data protection safeguards.

2.9.6. EDPS Surveys

During 2021, the DPO took an active role in the contribution of Europol's replies to a COVID-19 related survey with the aim of mapping the processing activities and tools used by all EU institutions, agencies and bodies to ensure business continuity in times of COVID-19 and to gather information as to how compliance with the data protection requirements under Article 8 of the Charter of Fundamental Rights and Regulation 2018/1725 is ensured. The survey focuses on three areas: new processing operations implemented by EUIs as part of their return to work strategy; IT tools or solutions implemented or enhanced by EUIs to ensure business continuity in times of telework and new processing operations implemented by EUIs in charge of public health related tasks. The launch of the survey raised internal discussions on various topics concerning the lawful processing of personal data in COVID-19 and served as an awareness raising tool on the importance of ensuring that despite the COVID-19 situation, all new processing operations shall be compliant and respect people's right to privacy and data protection.

The DPO, furthermore, contributed to the EDPS survey on the '**Report on the application of Regulation (EU) 2018/1725 (EUDPR) - collection of feedback from EU institutions, bodies, offices and agencies**'. The survey aimed to collect information from all the EU institutions, bodies and agencies subject to the Regulation 2018/1725 in order to provide information to the report in accordance with Article 97 of it stipulating that the Commission shall prepare regular reports on its application.

2.9.7. EDPS related public access requests

The DPF also played its role in responding to requests by the EDPS addressed to Europol as third party regarding public access requests addressed to Europol's external data protection supervisory authority. In 2021 the DPF accompanied two EDPS consultations of Europol related information.

3. EUROPOL REGULATION RECAST

In response to pressing operational needs and calls by the EU Member States for stronger support by Europol, the Commission Work Programme for 2020 announced a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation". Throughout 2021 the DPO continued to contribute to the debate.

This included a written contribution to the Management Board in March elaborating on biometric data as sensitive personal data and prior consultation of the EDPS.

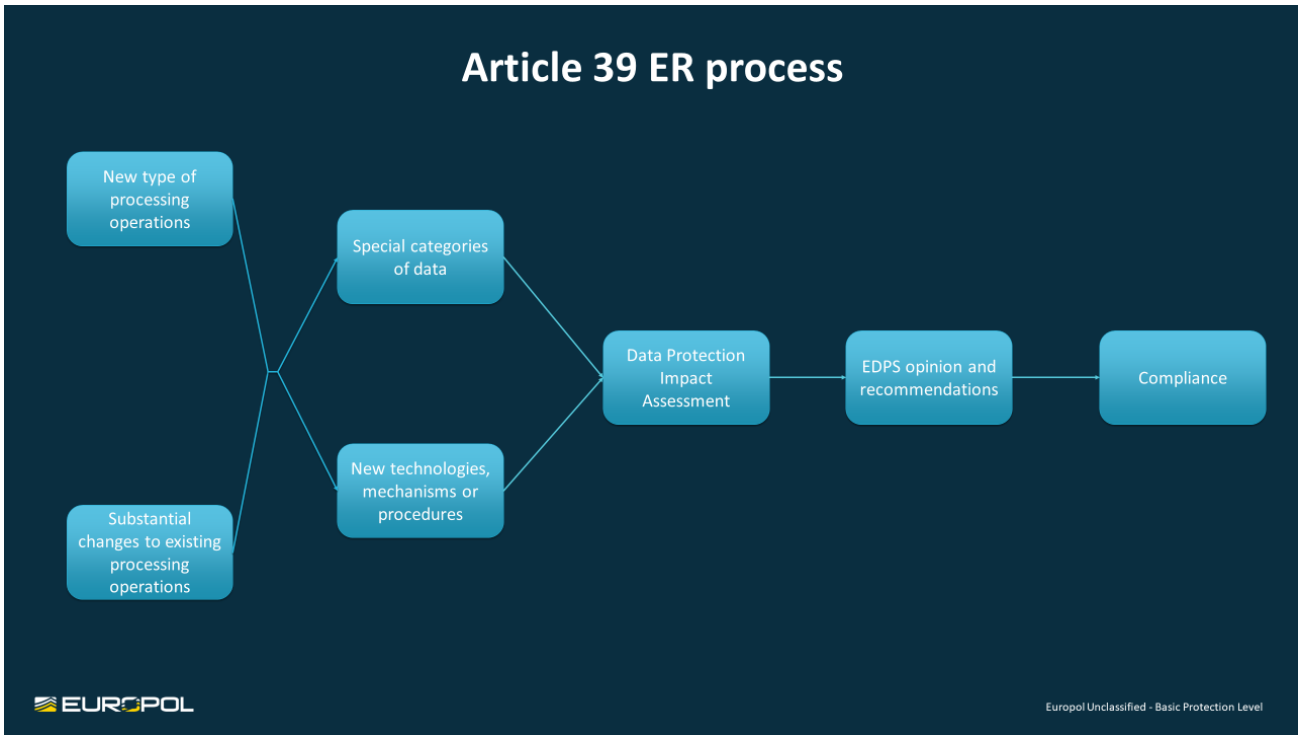
Furthermore, the DPO was requested to provide the Management Board Working Group on Corporate Matters in May with an assessment regarding a public opinion by the European Data Protection Supervisor (EDPS) on the Europol Regulation recast issued on 8 March 2021.

4. OPERATIONAL DATA PROTECTION

Also in 2021 the major part of DPF activities focussed on operational data protection matters. The workload remained high *inter alia* due to prior consultations of the EDPS according to Article 39 ER including the development and use of machine learning tools for the support of operational analysis, the further handling of Europol's so-called *big data challenge* as well as a continuously high level of data subject access requests.

4.1. Prior Consultation of the EDPS on new Types of Processing Operations

New types of processing operations that include processing of sensitive categories of personal data or data that present a specific risk for the fundamental rights and freedoms of data subjects and that have been launched or substantially changed after 1 May 2017 are subject to prior consultation by the European Data Protection Supervisor (EDPS) in accordance with Article 39 ER. Special (sensitive) categories of data as referred to in Article 30(2) ER are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life.



The tool used to implement the process of prior consultation is the so-called Data Protection Impact Assessment (DPIA). The DPIA as a tool analyses and controls the risks stemming from the processing operation.[5]

Touching upon a risk-based approach to data processing as well as documentation of processing operations, carrying out a DPIA is not mandatory for every processing operation.[6] In accordance with Article 39 ER, a DPIA and respectively formal prior consultation process is legally required when:

1. There is a ***new type of processing operation that includes the processing of special categories of data as referred to in Article 30(2) ER***;
2. There is a ***new type of processing operation*** where the type of processing, in particular using new technologies, mechanisms or procedures, ***presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects***.

What this means in practice is that there is no legal requirement for prior consultation when there is:(i) no new type of processing operation (processing operation that have been launched or substantially changed after 1 May 2017); (ii) no new type of processing operation that includes the processing of sensitive personal data; and, (iii) no new type of processing operation that presents specific risks for the fundamental rights and freedoms, in particular the protection of personal data, of data subjects.

[5] EDPS, *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (v.1.3 July 2019), p. 3.

[6] EDPS, *Accountability on the ground Part I: Records, registers and when to do Data Protection Impact Assessments* (v.1.3 July 2019), p. 9.

The Article 39 threshold under the Europol Regulation is rather low in contrast to other comparable legal frameworks.[7] Europol Regulation talks about "specific risks" whereas the DPIA/prior consultation mechanism under for instance Regulation 2018/1725 refers to the need for a DPIA for processing operations that are likely to pose a "high risk to the rights and freedom of data subjects" and prior consultation for "high residual risks" in the context of Article 39(1) Regulation 2018/1725.[8]

In the context of Article 39, the DPF has established and documented the respective process in close consultation with all Europol Directorates. In practice, the data controller brings to the attention of the DPF all initiatives that involve the processing of personal data and may hence require a prior consultation by the EDPS. The DPF includes these processing operations into the Article 39 section of the inventory of operational processing activities.[9]

By way of filling in a questionnaire, the respective data controllers carry out the Data Protection Impact Assessment (DPIA). The DPF reviews the DPIA with the aim to propose data protection safeguards but also in terms of the legal requirement to prior consult the EDPS. If the processing operation reaches the threshold of prior consultation, the DPF makes sure that all exchanges of information and communication between the controller and the supervisory authority in the context of Article 39 ER are duly registered. In this regard, the DPF acts as the link between Europol and the supervisory authority. Additionally, all EDPS recommendations resulting from EDPS Article 39 prior consultation opinions are included as part of the DPF compliance tool.

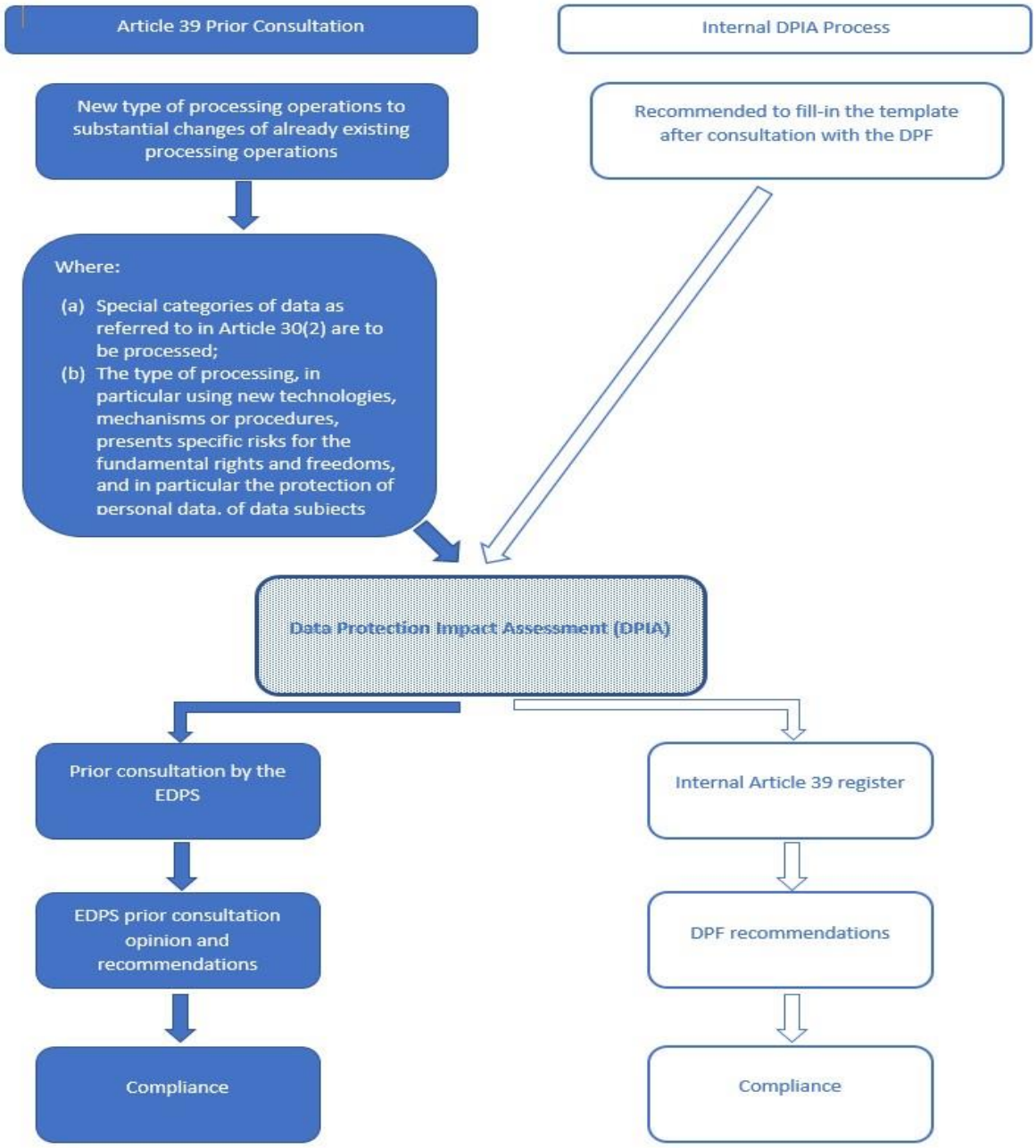
In the alternative scenario, i.e. in cases in which the processing operations presented to DPF do not require full-fledged prior consultation of the EDPS, the DPF has established an identically robust process. The DPF advices the data controller on the completion of the whole data protection risk assessment regardless. Once done, all internal DPIAs for processing operations, which do not fulfil the criteria for prior consultation under Article 39 ER, are filed in an internal DPIA register. Furthermore, an additional internal follow-up procedure has been established on part of the DPF to oversee the potential evolvement of the processing operations and their future Article 39 ER implications if any.

The 'internal' and 'external' DPIA process established by Europol can best be exemplified as per the diagram below:

[7] Article 39 and 40 Regulation (EU) 2018/1725; EDPS, *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (v.1.3 July 2019), p. 3; EDPS, *Accountability on the ground Part I: Records, registers and when to do Data Protection Impact Assessments* (v.1.3 July 2019), p. 9.

[8] Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725, Recital paras 2 and 3.

[9] Inventory of operational processing operations process description, EDOC#1166509.



In addition to the established above process, the DPF has been working on raising awareness among Europol Directorates regarding the legal obligations in light of Article 39 ER. Regular awareness sessions are organised by the DPF. Besides, updates are provided to the DEDM meetings as well as regular reporting to the Management Board.

In the second half of 2021, the DPF updated the Guidelines on the implementation of Article 39 for internal Europol use.[10]

4.1.1. Internal DPIAs process

In 2021, the DPF has received 3 internal DPIAs, namely:

[10] DPF Article 39 Guidelines, EDOC#987546

- OTF Limit LIVE Phase
- OTF Greenlight LIVE Phase
- Cross Domain Solution (CDS)

In the context of last bimonthly meeting with the EDPS for 2021 (namely, the meeting on 03/12/2021), the data controller together with the DPF presented the internal CDS DPIA to the EDPS team. The idea behind the presentation was to present the supervisor with Europol's position on why the CDS is not to be considered as falling under the ambit of Article 39. The final EDPS position on the matter is currently expected.

4.1.2. Formal Article 39 prior consultation procedure

Until the end of 2021, three full-fledged prior consultation opinions have been received:

- Europol's Access to VIS Data (EDPS Opinion: 01/03/2021)
- Machine Learning Toolbox (EDPS Opinion: 05/03/2021)
- Data Management Portal (EDPS Opinion: 05/11/2021)

In particular, both 'Europol's Access to VIS Data' and 'Machine Learning Toolbox' prior consultation opinions are to be considered as 'conditional' – the supervisor put forward lists of requirements that have to be met prior to the start of the processing operations. Additionally, on the occasions of both opinions, the EDPS stresses that with regards to future prior consultations, the EDPS expects that Europol:

(i) provides a data flow diagram for each purpose of the processing to fully clarify the legal framework in which it operates;
(ii) includes in the process all applicable control measures; and,
(iii) specifically describes the scenarios that would trigger the process under consultation and to indicate any processes interacting with the process at stake.

This additional set of information and documentation has to be provided in addition to the already established Article 39 notification (containing the DPIA), risk assessment table (including impact on data subjects), process description and description of the infrastructure used. This latest additional request for documentation can also cause delays in terms of the preparation of the process and the actual implementation. Nevertheless, the DPF is working closely with data controllers in order to provide the EDPS with the fullest possible package of documentation from the outset of the processing operations. DPF also regularly stresses that this is also in line with the operational interests of data controllers.

The most recent prior consultation opinion on Europol's Data Management Portal (DMP)[11] is a peculiar one as it introduces a couple of new requirements on part of Europol. For instance, for the first time since the implementation of the provision in 2017, Europol is required to report on the status of implementation of the three issued recommendations within one month of the date on which the prior consultation opinion is issued. This tight deadline was difficult to be met on the side of the data controller and therefore a request for extension was requested by the supervisory authority. The request has been granted and the data controller submitted their input within the newly set deadlines.

4.1.3. Machine learning toolbox

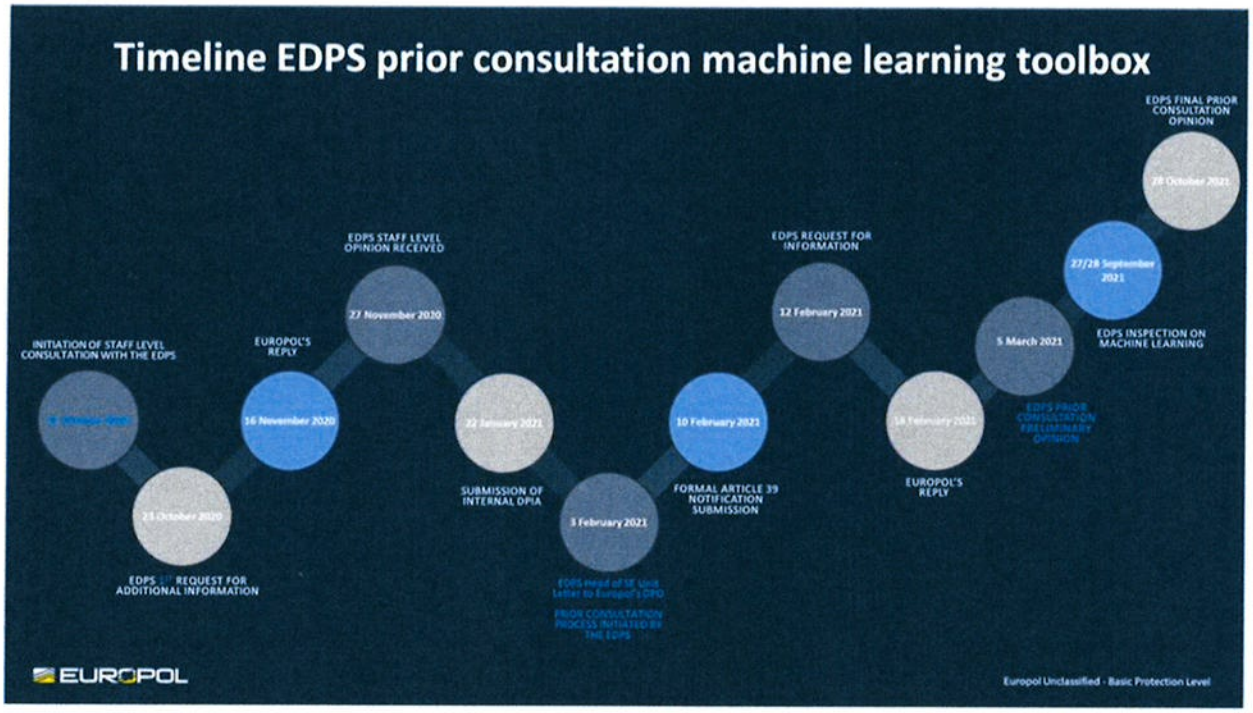
The machine learning toolbox has been developed in order to support the analysis of huge and complex amounts of information in the context of [redacted]

[11] Article 39 prior consultation opinion on Europol's Data Management Portal (DMP), EDOC#1196409.

[redacted] as well as similar already ongoing or future investigations supported by Europol (e.g. [redacted]).

By letter dated 28 October 2021 the EDPS provided Europol with an opinion ultimately allowing for the use of operational personal data for the development and validation of machine learning tools to support operational analysis. The EDPS in this context explicitly thanked Europol for the constructive approach and collaborative spirit shown by staff.

The EDPS opinion formulates five conditions mainly referring to documentation requirements and demands regular meetings at staff level in order to discuss and follow-up on the related Data Protection Impact Assessments (DPIAs). While this EDPS letter is a crucial step *forward* and the basis for initiating the necessary processing operations upon personal data in full compliance with the principle of data protection by design, it should be noted that the timeline to achieve this outcome lasted more than one year. A more detailed overview can be found in the following visual:



Europol is likely the first EU agency that already has an approved policy in place in this area. This demonstrates that the agency is mindful of the sensitivity of the use of AI systems by law enforcement agencies and conscious of the fact these tools must be designed, built and trained in a manner which fully respects European data protection and human rights standards and follow the ethical guidelines for trustworthy AI.

4.2. Europol's Big Data Challenge

One of the data protection related main topics also throughout 2021 was Europol's so called *big data challenge*. The issue had been raised internally by the DPF and subsequently pro-actively brought to the attention of the Supervisor during a high level meeting between the Executive Director (accompanied by the DPO) and the EDPS held

on 1 April 2019. Reference is made to the DPO Annual Reports 2019 and 2020 for further background including the EDPS admonishment issued to Europol on 17 September 2020 and the Action Plan provided by Europol in response on 17 November 2020.

On 4 December 2020, the EDPS provided comments on the Action Plan, and requested further clarifications on a number of elements. On 17 March 2021, Europol sent a Progress Report detailing the state-of-play concerning measures being put in place under the Action Plan.

The Management Board discussed the importance of the subject matter in all meetings in 2021. Particular focus was on the operational impact of a potential EDPS order to Europol to carry out the destruction of datasets.

Throughout 2021 the DPF supported the agency in implementing the EDPS decisions and the communication with the EDPS specifically regarding the requested three-monthly reporting to the EDPS with particular focus on the further development of the Data Management Portal (DMP) as well as NEO developments considering the links drawn by the EDPS to these initiatives making reference to the Action Plan and related progress reports.

4.3. Brexit

Another aspect that continued to cause additional workload for the DPF also throughout 2021 was the further implementation of the Brexit, in particular, the practical consequences of the UK's withdrawal that apply at Europol as of 1 January 2021.

To ensure a smooth transition of the operational cooperation with the UK after the transition period has ended, the MB, in agreement with the EDPS, adopted a decision pursuant to Art. 25(6) ER authorising a set of transfers to the UK (EDOC#1054168). The DPF was substantially involved in the drafting of the decision and its consultation with the EDPS.

The MB Decision on the set of transfers envisaged the need to continue ensuring a lawful and proportionate exchange of personal data between UK and Europol, taking note of the volume of the exchange of personal data and the corresponding need of data protection safeguards. The additional data protection safeguards as defined in the MB Decision include the necessity to establish the proportionality and necessity of the transfers of personal data which is also implemented via the overview of cases maintained by the Operations Department; restrictions on the processing of special categories of persons and sensitive personal data; application of the restrictions and safeguards to the transfers as anticipated in the Europol Regulation; maintaining a list of cases with the involvement of UK; SIENA disclaimer attached to all transfers of personal data to UK, etc.

The DPF continued supporting the agency in the drafting of the working/administrative arrangement that was signed by Europol and the UK in the second half of September 2021. The DPO took part in the negotiations on the working arrangement with the UK. The EDPS has been also consulted in the process.

In the meantime, the Commission has on 28 June 2021 adopted two adequacy decisions for the United Kingdom - one under the GDPR and the other for the Law Enforcement Directive. The exchange of personal data between Europol and the UK can since then be based on Article 25(1)(a) ER.

4.4. EU Interoperability

Throughout 2021 the DPF also supported Europol in the further implementation of the interoperability principle. Following the endorsement of the Europol Roadmap on Interoperability, a "Europol plan for the implementation of the new EU information systems architecture (EU Interoperability)", also known as the "Europol EU Interoperability Plan", has been drafted and is being maintained to further detail and update the Roadmap. The purpose of the Implementation Plan is to provide an up-to-date and detailed overview of activities required by Europol for the implementation of the Interoperability Agenda.

The EU Interoperability Europol Programme is chaired by Europol Deputy Executive Director Capabilities (DEDC). In addition to the Programme Board, experts from all three directorates of Europol and the DPF come together in the form of EU Interoperability Working Body to discuss topics of relevance.

The DPF has been involved from the outset in the EU Interoperability Working Body at Europol. The timely DPF involvement has added value to the materialisation of the interoperability planning at Europol. The DPF involvement in this particular overall interoperability project is one of the best examples of the proactive implementation of the principles of data protection by design and by default in practice.

4.5. Operational and Analysis Centre (OAC)

Throughout 2021 the DPF actively supported the Operational and Analysis Centre (OAC) in ensuring data protection compliance. The OAC provides Member States as well as their Liaison Bureaux, Europol associated partners and internal operational and strategic stakeholders with a set of cross-cutting services and capabilities to support police investigations and information sharing, including several functions of operational and strategic nature. In particular, the OAC acts as the central information hub and gateway of all operational information and intelligence channelled through Europol.

O1-24 is the particular organisational unit within the OAC mandated to develop and enforce standards in the processing of operational information, both for data quality and data protection, and act as a contact point for data protection matters. O1-24 serves as a second level of assurance in the Operations Department.

In the context of Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge' the organisation informed its external data protection supervisory authority of the appointment in June 2020 of a Data Quality Control Coordinator for Europol's Operations Directorate. The Data Quality Control Coordinator is placed in O1-24 and his work is to ensure the implementation of the current data review mechanism and that data processing is performed in line with the ER, in particular Annex II.

The Data Quality Control Coordinator was positioned to work in close cooperation with the DPO and produce a monthly progress reporting on the enhanced data review activities with particular attention to the labelling of specific files, the compliance with access rights, including the rejection and deletion of data. In November 2021, Europol decided to use two of its new positions in 2022 for two additional staff members on data quality control in the Operations Directorate. Within the Analysis and Strategic Coordination Unit, three staff members (the Data Quality Control Coordinator plus the two new positions) will be working full time on data review, control, compliance and quality. These posts are in addition to data quality control as a daily task of every analyst and data specialist in the organisation. Depending on the recruitment procedures

and availability of the recruited staff, it is expected that the extra staff will be available latest by September 2022.

Europol also decided on the establishment of a dedicated task force in the Operations Directorate (OD) to ensure the implementation of the Action Plan. The DPF was invited to participate in this task force during a meeting held on 10/01/22 presenting its analysis of the EDPS decision on the retention by Europol of datasets lacking Data Subject Categorisation (DSC).

A summary of the progress reporting regarding the Action Plan was announced to be made available to the EDPS on a quarterly basis. Progress reports on the Action Plan as a whole were submitted to the EDPS in March as well as in October 2021. The third progress report was being finalised in January 2022.

4.6. European Serious Organised Crime Centre (ESOCC)

Throughout 2021 the DPF actively supported the Serious Organised Crime Centre (ESOCC) in ensuring data protection compliance. ESOCC is the main entity within the organisation to deliver work of Europol in the fight against serious and organised crime. This includes providing operational support to the EU Member States in investigations related to priority and investigations on high-value targets, coordinating the implementation of the standard operating procedure on the selection of high-value targets and the establishment of operational task forces (OTFs) in Europol, supporting the EU Member States in the implementation of the operational activities related to the EU Policy Cycle as well as supporting strategic analysis by providing expertise and substantive contributions to improve the intelligence picture in specific crime areas and on organised crime groups (OCGs).

ESOCC also includes the European Migrant Smuggling Centre (EMSC) which encompasses Europol's work on criminal activities related to irregular migration. The goal of the EMSC is to have a decisive role in proactively supporting EU Member States to target and dismantle organised crime networks involved in migrant smuggling, with special attention provided to existing and emerging EU hotspots. From 2017, particular focus has been placed on the Central Mediterranean area in line with the Implementation Plan stemming from the Malta Declaration on migration. A closely linked dedicated analysis project on Trafficking in Human Beings deals with different forms of human exploitation.

The DPF has, furthermore, been involved in the preparations of an amendment of the opening order portfolio rearranging the analysis project (AP) structure in a way to address identified operational business needs while further facilitating information management. The idea is to merge the currently existing APs Cannabis, Heroin, Synthetic into a single drugs related analysis project AP DRUG CRIME. Furthermore, AP High Risk Organized Crime Groups would in future also encompass the other crime group focussed analysis projects AP ITOC, EEOC, Monitor and Copper.

The expected debate on this amendment proposal will from a data protection perspective first and foremost be focussed on the so called purpose limitation principle. This means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (see Article 28(1)(b) ER).

The opening orders are an implementation of this principle in the sense that they determine which personal data exactly may be processed for the purpose of the specific analysis project. As you know, each opening order to that end entails a data category table. Where it becomes apparent that personal data may be relevant for another operational analysis project, further processing of that personal data shall only be permitted insofar as such further processing is necessary and proportionate and the personal data are compatible with the respective other data category table (see Article 18(2)(b) ER).

Europol currently has 32 APs. One could hence translate this into a "purpose limitation factor" currently amounting to 32. The considered reform would arguably bring the portfolio down to 25 APs potentially triggering concerns of weakening the purpose limitation factor by the value of 7.

However, an important argument is that all drugs related APs in any case largely have the same or at least very similar data category tables. The impact on the purpose limitation principle would in this scenario not be significant as an allocation of personal data from one drugs related AP to another drugs related AP would in any case almost always comply with the above outlined requirement derived from Article 18(2)(b) ER).

During 2021, the DPF continued its close involvement in ensuring data protection compliance of Europol's requests for PNR data or the result of processing those data from the PIUs of Member States within the limits of its competences and for the performance of its tasks under Article 10 of the PNR Directive. The DPF is involved in the discussions on setting data retention periods in SIENA following PIUs' requests.

4.7. European Cybercrime Centre (EC3)

Throughout 2021 the DPF actively supported the European Cybercrime Centre (EC3) in ensuring data protection compliance. The aim of EC3 at Europol is to strengthen the law enforcement response to cybercrime in the EU and to help protect European citizens, businesses and governments. The core areas of expertise of EC3 are to strengthen and integrate operational and analytical capacities for cybercrime investigations in the EU, including a reinforcement of the cooperation with EU Member States, international partners and the private sector and to evaluate and monitor existing preventive and investigative measures in the area of cybercrime. Furthermore, EC3 supports the development of training and awareness-raising initiatives of law enforcement, judicial authorities and the private sector.

The quarterly meetings between the DPF and the Head of EC3 continued also in 2021 and were used to mutually raise awareness on upcoming issues and identified concerns. These meetings can be seen as an expression of the shared view regarding the importance of maintaining a good data protection posture.

Members of EC3 were also actively involved in the 7th EDEN Conference participating in panels dealing with the human factor in Artificial Intelligence and future trends in cybersecurity and data protection. The panellists debated real life examples of the use of contemporary technologies and related data protection challenges for law enforcement.

The DPF, furthermore, continued to support EC3's involvement in the H2020 GRACE project from a data protection perspective. GRACE is an acronym for 'Global Response Against Child Exploitation' and the project looks at efficiency gains in digital forensics in the context of criminal investigations into child sexual abuse.

The GRACE project has on 1 February 2021 also been discussed in the Joint Parliamentary Scrutiny Group (JPSG), in particular, during the panel session featuring the ED as well as the EDPS. Several Members of the European Parliament (MEP) have raised their concerns with regard to the use of AI and machine learning techniques by

Europol with one MEP also specifically making reference to Europol's involvement in H2020 projects including GRACE.

The DPF was, furthermore, involved in the assessment of a potential transfer of personal data from AP TWINS to a third country with which Europol does not have an operational cooperation agreement. In the absence of both, a Commission adequacy decision and an agreement according to Article 218 TFEU, only an exceptional transfer according to Article 25(5) ER could be considered.

The example showed that reconciling the various interests at stake can be extremely difficult. Europol supported a case concerning an individual suspected of serious sexual abuse of an unknown number of minors. The dilemma between safeguarding the vital interests of victims of child sexual abuse on the one hand and serious risks of fundamental rights violations of the suspect on the other, including imposition of the death penalty without application of proceedings in respect of the rule of law became very apparent.

The DPF recommended that the Executive Director could consider seeking assurance from those third country authorities that principles of a fair trial will be respected and the imposition of the death penalty excluded, before submitting the personal data in question. The transfer was ultimately not executed given consultations with Member States as contributors of the underlying personal data were still ongoing including with a view to the worrying broader fundamental rights situation in the third country concerned.

4.8. European Counter Terrorism Centre (ECTC)

Throughout 2021 the DPF actively supported the European Counter Terrorism Centre (ECTC) in ensuring data protection compliance. ECTC was created in January 2016 as a hub of expertise that reflects the growing need for the EU to strengthen its response to terrorism *inter alia* by sharing intelligence and expertise on terrorism financing (through the Terrorist Finance Tracking Programme (TFTP)) and to counter online terrorist propaganda and extremism through the EU Internet Referral Unit (EU IRU).

The ECTC's principal task is to provide operational support to EU Member States in investigations following terrorist attacks. It cross-checks live operational data against the data Europol already has, quickly bringing financial leads to light, and analyses all available investigative details to assist in compiling a structured picture of the terrorist network.

The DPF inter alia supported the Sirius Project in the drafting of guidelines for online service providers regarding cross-border requests by law enforcement authorities for electronic evidence. The Sirius Project is co-implemented by Europol and Eurojust and serves as a central reference point in the EU for knowledge sharing in the field of electronic evidence, offering a variety of services, such as guidelines, training and tools and bringing together a community of EU competent authorities expert in the field of cross-border access to electronic evidence.

The so called voluntary cooperation by online service providers with law enforcement authorities plays an important role in practice which is why the Sirius Project took the initiative to draft said guidelines as well as a compendium of OSPs policies on cross-border requests for electronic evidence. The DPF was consulted to assist in assessing data protection implications.

The question of lawfulness of data processing by online service providers is to be assessed in light of Article 6 GDPR which in paragraph 1(f) states that processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the

controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Recital 50 GDPR is interesting in this context as it reads:

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

An example in this regard would for instance be Article 15 ePrivacy Directive stipulating that stipulates:

Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

The data controller and DPF also liaised with the Data Protection Office at Eurojust in order to further clarify the underlying complex matter to the extent possible. The DPF, furthermore, initiated a consultation of the EDPS considering that the EDPS shall act in close cooperation with the national supervisory authorities on issues requiring national involvement. Given the nature of the request and the division of competences on this issue, the EDPS shared the documents with the Europol Cooperation Board (ECB) and with the Coordinated Supervision Committee (for input of national DPAs supervising Eurojust) to check whether they have specific comments or recommendations to make on the guidance. The data controller supported by the DPF was also invited to present the matter during a meeting of the ECB in November. To date, no additional guidance on the two presented documents has been received.

The DPO, furthermore, continued to support ECTC in the data protection compliant implementation of Europol's role in the TFTP. The DPO provided his advice on the verification of all Article 4 requests throughout the year. In addition, the DPO contributed to the continued implementation of EDPS recommendations by providing advice regarding the requested adjustments of the TFTP process description.[12]

[12] See https://edps.europa.eu/data-protection/our-work/publications/inspections/edps-inpection-report-tftp_en, accessed on 18/02/21

4.9. European Financial and Economic Crime Centre (EFECC)

The European Financial and Economic Crime Centre (EFECC) launched its activities in June 2020. EFECC aims to enhance the operational support provided to EU Member States and EU bodies in the field of financial and economic crime. It promotes the systematic use of financial investigations and forms partnerships with public and private entities in order to trace, seize and confiscate criminal assets in the EU and outside.

This involves improving the exploitation of financial intelligence across the EU, engaging with non-EU countries and organisations, in order to make the best use of the provisions allowing access to financial information in the EU or under the relevant national legislation.

In this context, 'financial intelligence' consists of the suspicious transaction reports and other information relevant to money laundering and associated predicate offences. The analysis and dissemination of financial intelligence supports the identification of criminal networks, the tracing of proceeds of crime and assets potentially subject to seizure and confiscation, as well as the collection of evidence for criminal proceedings.

As with the other centres of expertise hosted at Europol, data protection plays an integral part of the activities of EFECC as well.

In particular, the DPF supported EFECC throughout 2021 in the handling of a processing ban issued by the EDPS on 20 December 2019 regarding the possibility for the agency to act as technical administrator of FIU.net (EDOC #1088295, EDOC #1088298). This is the first time that Europol's external data protection supervisory authority makes use of its enforcement powers according to Article 43(3)(f) ER.

The ban concerned "(…) all processing by Europol of data related to individuals who are not classed as "suspects" under the applicable national criminal procedure law (…)." Making reference to the crucial role of FIU.net in the fight against money laundering and terrorism financing, the EDPS, however, "suspends" the ban for a period of one year from the day of this decision "(…) in order to allow Europol to ensure a smooth transition of the technical administration of FIU .net to another entity".

During this transition period the EDPS asked Europol to report every two months on the steps taken to achieve such transfer. Europol provided the respective reports to the EDPS[13]. The DPF supported the data controller in drafting altogether 14 reports.

Specifically, in order for FIU.net to be safely and securely transferred to the Commission, the infrastructure at the Commission datacentre had to be set up in a way that facilitated a smooth migration of the system, involving procurement of new hardware and thorough testing. Based on the estimation of the Commission, it was both parties' view that this infrastructure could be ready in May 2021, following which a progressive set-up, test, and migration of FIU.net could be carried out over a period of several months, with the migration finalised at the latest in the course of September 2021. A respective prolongation of the suspension of the processing ban was consequently requested by both parties and also granted by the EDPS.

Europol successfully completed its activities related to the technical transfer of the FIUs' FIU.net nodes to DG FISMA/OLAF and seized operating as the technical administrator of the FIU.net system anymore in line with the prolonged suspension period.

[13] EDOC #1098478, EDOC #1107388, EDOC #1115170, EDOC #1127256 and EDOC #1138758.

4.10. Assurance Activities

In 2021 the DPO continued to implement its assurance function by means of real-time monitoring of compliance with the Unified Audit Solution (UAS) alerting functionality and other forms of compliance checks.

The advantage of this approach is an increase in flexibility as well as a cut of red tape as compared to formal audit reporting. Compliance checks can take various forms ranging from spontaneous checks of the operational systems to a follow-up phone call to address identified issues on-the-spot. However, they can also result in a formal report to the controller in order to flag identified issues and provide structural recommendations for improvement.

In comparison to formal audits, the data protection compliance checks performed by the DPO as second line assurance function do not have to adhere to any strict protocol of auditing standards, but can be tailored in order to serve the best purpose of improving processing operations with the goal to add value. For instance, a formal audit by default includes an interview of the auditee which is sometimes time consuming and binding operational resources. A compliance check can skip this step if there is a common understanding regarding relevant facts and a solution for identified issues already envisaged.

The aim remains to provide relevant stakeholders including Europol's management with an assessment of the level of compliance with applicable data protection rules.

In the operational domain the assurance activities in 2021 included random as well as targeted checks of personal data exchange via SIENA, checks of soft deleted data older than 1 month, checks of UK data in the EIS, checks of EncroChat data and personal data relating to minors, a check of an EU IRU as well as a digital forensic report in the context of a witness statements, a check whether EUNavCen satellite imagery and complementary information provided to Europol include personal data as well as a formal DPF Compliance Check Report regarding the FACE application.

4.11. Exercise of Data Subject Rights

Any data subject has a right of access to personal data concerning him or her, a right to rectification if those data are inaccurate, and a right to erasure or restriction if those data are no longer required. The rights of the data subject and the exercise of such rights shall not affect the obligations incumbent upon Europol and shall be subject to the restrictions laid down in the ER.

The DPF takes care of the right of access and the right to rectification, erasure and restriction addressed to Europol in accordance with the procedure laid down in the Guidelines issued by the DPO on the individual right of access (EDOC#948181), the process description on handling of data subject access requests (EDOC#942111), the advice provided by the EDPS and the best practices in exercise of data subject rights.

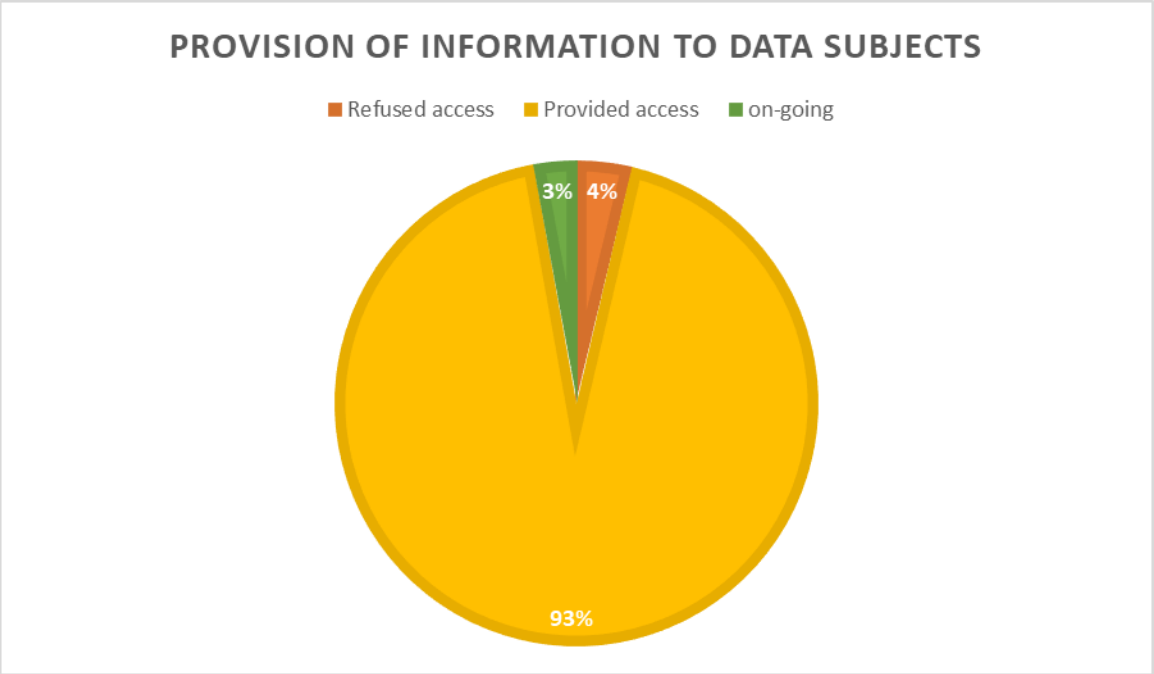
Article 36 ER states that any person shall have the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol.

4.11.1. Statistics

During 2021, Europol received a total of 353 data subject access requests. Despite the lower number of requests compared to the previous year (513 in the course of 2020), the workload in the handling of data subject access requests increased significantly due

to the increased number of full hits and the required enhanced cooperation with the EDPS.

In line with the established practice, when there is no data about the requester in Europol's systems, the DPF informs him/her accordingly[14]. As it can be seen from the tables below, Europol granted access to information in 93% of the received requests which underlines the applied transparency towards data subjects whenever possible in line with the applicable rules.



When there is a hit in Europol's system, the DPF launches the consultation procedure with the competent authorities of the EU Member States concerned and the provider of the data concerned.

In handling the 32 full hits on data subject access requests, the DPF launched more than 50 consultation procedures on the provision of response to the data subjects.[15] During 2021, the ED took note of all the objections expressed by the EU Member States concerned and refused access to the provision of information in all instances where an objection was duly justified in accordance with Article 36 (6) ER.

In 2021, there were in total 32 full hits out of the total 353 requests (almost 10% of all). In comparison, in 2020, there were 26 full hits out of 513 (5 %of all). In 2019, there were 10 full hits out of 321 (3% of all). In 2018, there were 12 full hits out of 524 (5% of all).

[14] Article 36 (2) ER sets, without prejudice to Article 36 (5), sets the information requirements for Europol's answer

[15] *Due to the fact that data subjects are often contributed by various Member States and providers of data concerned.*

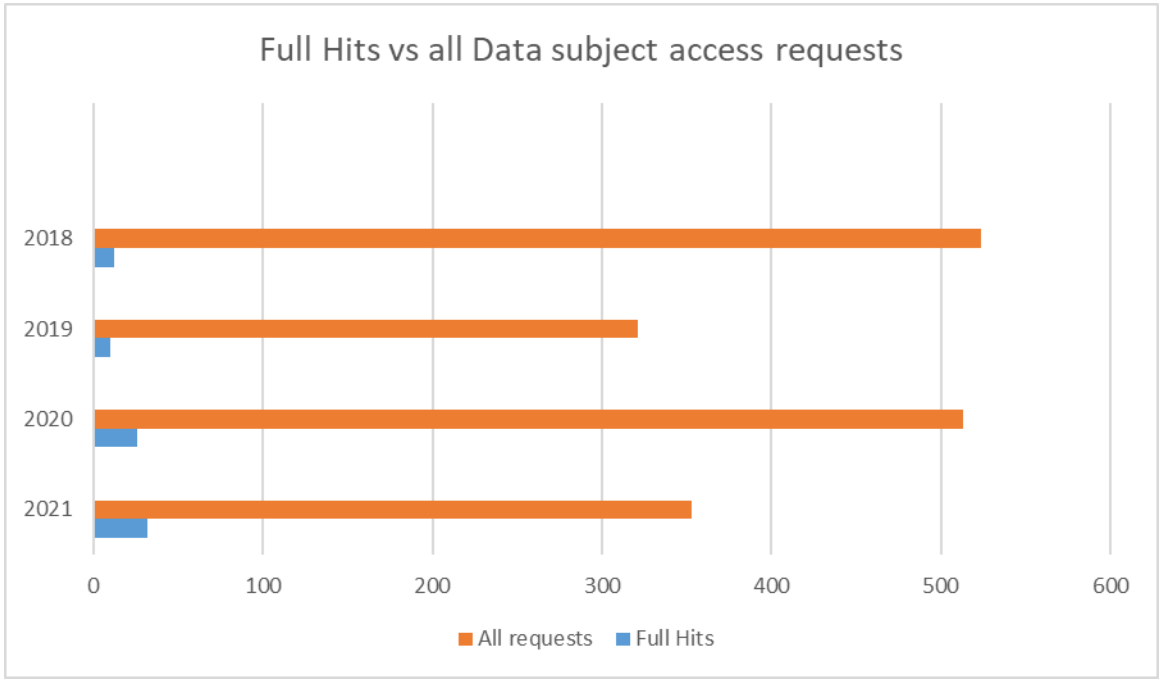
The distribution of data subject access requests per EU Member State is the following:

317	Germany
14	Austria
9	Sent directly to Europol
4	The Netherlands
3	Belgium
2	Finland
1	Slovenia
1	Spain
1	Czech Republic
1	Cyprus

Most of data subject access requests are received from Germany via its competent national authority (89% of all requests). However, it should be noted that the landscape of receiving EU Member States is changing and it is wider than before. It is expected that this trend will grow.

4.11.2. DPF workload implications

The increase of full hits on data subject access requests doubled compared to previous years which has a serious impact on the DPF workload related with the handling of data subject access requests.



In addition, the diverse criminal activities of members of organised criminal groups requesting access to information in accordance with Article 36 ER required engaging

additional stakeholders in the consultation procedure on Europol's reply. Due to the rapidly changing situation in the context of investigation procedures among different EU Member States, which might have an impact on the proposed answers to data subjects, the contacts between the DPF and relevant Liaison Bureaux were more frequent. All steps taken by the DPF in this process (meetings with the Liaisons Officers, contacts with analysts, communication with competent national authorities) are duly documented in order to demonstrate the reasons on which a decision on the exercise of a right of access is based and to answer the EDPS increased demands on the formalisation of the procedure.

4.11.3. Consultation procedures

Two consultation procedures were launched with the EDPS in relation to data subject access requests during 2021. As an answer to a consultation procedure launched with the EDPS in 2020, in relation to the exercise of data subject access via the competent national authority of UK after Brexit, the DPF took follow-up actions in the beginning of 2021. The EDPS replied to the consultation procedure that UK data subject access requests received as from 1 January 2021 should be handled according to the existing procedure established under the ER for third countries (EDPS Case no. 2020-0937). The DPF ensured the proper implementation of the recommendation provided by the EDPS in its opinion on UK Data Subject Access Requests (Case 2020-0937 -EDOC 1139199). The EDPS recommended that Europol takes steps to ensure that relevant counterparts (e.g. the competent authorities of the UK as well as the 27 Member States who may need to transmit UK requests in the future) are duly informed of the changes in this regard. As a follow-up action, the DPO sent a letter (EDOC#1170707) to the Liaison Bureau United Kingdom informing them that according to Article 36(3) of the Europol Regulation, data subjects desiring access to their data must make a request 'to the authority appointed for that purpose in a Member State of his/her choice.

On 31 March 2021, the DPF requested EDPS guidance on the notion of *reasonable intervals* according to Article 36 (1) of the Europol Regulation. The background of the request was the receipt of several repetitive data subject access requests from citizens. It is important for Europol to have certainty about the period necessary to pass in order to consider a repetitive request being made at a reasonable interval and therefore treated as a new data subject access request under Article 36 of the Europol Regulation. The answer to what should be considered as a *reasonable interval* is particularly important in relation data subject access requests that result in full hits in Europol's systems and potentially will be brought to the attention to the EDPS by way of an appeals procedure. It requires clarification whether, in case of a repetitive request considered as a new one, Europol should launch again the entire consultation procedure with the Member States and the providers of the data concerned, or it would be possible that Europol relies on the assessment previously made and respond in the same manner.

On 13 July 2021, the DPF received the EDPS opinion on the notion of *reasonable intervals* which confirms the data protection compliance of the existing practice at Europol on the handling of repeated data subject access requests and provides recommendations on how to further ensure Europol's accountability in this regard.
The EDPS established that data subject access requests should continue being handled on a case-by-case basis in the context in which they were made. The EDPS confirmed Europol's possibility to define a threshold (for instance, a three-month interval) in order to *flag* data subject access requests that may potentially be qualified as unreasonably repetitious. Those flagged requests, which fall below the threshold, should then be subject to a more detailed case-by-case assessment. When carrying out the assessment to determine if a reasonable interval has elapsed, the primary consideration should be the fact or probability that circumstances surrounding the related data processing have altered since the last request. An alteration may relate to a deletion of the data. It may

be occasioned by a previous no hit' becoming a hit due to previously non-searchable data having been extracted and included as an entity in Europol's systems. An alteration may also occur if access has previously been refused on the basis of a legal ground justifying the application of a restriction under Article 36(6) and the validity of that legal ground has since elapsed. All the decisions taken by Europol in relation to data subject access requests should be duly documented.

In 2019 the DPO launched a consultation with the EDPS on the internal procedure for handling data subject access requests and the approach towards partial hits in Europol's systems (EDPS Case no. 2019-0570). In particular, the DPO requested the EDPS whether the following systems should be checked on the basis of a data subject access request: *Check the Web,* Computer Forensic Network and SIS II. The consultation became necessary after it appeared that the EDPS has a different approach regarding the compliance of the handling of data subject access request then the Joint Supervisory Body and legal certainty for Europol was required.

It should be clarified that the practice of the DPF included checks in SIS II on data subjects made only in specific cases (where there was a clear indication in iBase SOC or Palantir that there is an European Arrest Warrant on the person) and in Check the Web, where there were reasonable grounds to believe that a content related to the requester was stored. However, the DPF has not run checks on data subjects in the CFN. The DPO also asked the EDPS how to treat the so-called *partial hits* in Europol's systems, in which Europol cannot determine whether personal data in Europol's systems is in fact related to the requester.

On 13/12/21, the EDPS issued an opinion on Europol's procedure to handle data subject access requests and sent it to the Data Protection Officer with a corresponding letter (EDOC#1204775). As explained by the EDPS, the delay was caused due to the fact that the consultation partially covered the inquiry on CFN.

The EDPS Opinion acknowledged the DPF practice on the handling of partial hits on data subject access as a robust procedure which includes cooperating with the contributing entity to verify the potential match. In addition, it is stated by the EDPS, that in cases of doubt on whether the requester is identical to the person in the systems, Europol must make only what is called reasonable efforts to clarify whether the personal data belong to the requester.

Taking into account the current status of CFN data protection compliance, the EDPS invited Europol examine whether any changes to the tools, structure or policies of the system could be made in order to allow (future) searches in CFN on the basis of data subject access requests in a less burdensome manner. Furthermore, the EDPS is of the opinion that the Check the Web portal should be included in Europol's searches in response to data subject access requests regardless of the fact that the frequency of any hits in that system is significantly lower. The EDPS acknowledged the practice of the DPF to perform limited checks in SIS II on data subject access requests, only when there are indications of European Arrest Warrant in Europol's systems. The DPO issued a briefing note with an initial assessment of the impact of the EDPS opinion on the internal handling of data subject access requests (EDOC#1214464).

4.11.4. Complaint cases

There are three on-going EDPS complaints cases on the decisions taken by Europol with regard to data subject access requests under Articles 36 and 37 ER. The EDPS has requested additional information concerning each complaint case. It should be noted that the requests of the EDPS for information concerning the cases are much more substantiated than before. The proceedings entail now a detailed and complete investigation of the actions taken by Europol with regard to the requests. These new

substantiated investigations of appeal cases by the unit dealing with complaints at the EDPS demonstrate once more the need to meticulously document the handling of data subject access requests at Europol.

As stated by the EDPS during the 10th JPSG meeting on 28/02/22[16], the increase in processing of large datasets by Europol will lead to increased quantities of unstructured data, including on individuals with no link to criminal activities. This will render the exercise of data subjects' rights both more critical and more complex.

5. ADMINISTRATIVE DATA PROTECTION

The activities in the area of administrative data processing continued to be marked by the pandemic and the processing of health data to prevent the spread of the disease together with the expansion of the activities of the Europol Medical Service. The DPF was substantially involved in the in various activities launched by the EDPS taken to monitoring compliance of Regulation 2018/1725[17].

5.1. Records of processing activities

A significant part of the activities taken by the DPF in the area of administrative data processing was dedicated to the provision of advice on ensuring the data protection compliance of new processing activities and currently on-going ones. The DPF provided guidance on 17 records of processing activities published in the internal register of records of processing activities in the course of 2021: Calls recording of general Europol phone number; Translation services; Processing of data of subscribers to the AIDA project newsletter; Meetings, events and conferences, hospitality, reception and travel arrangements data processing for Europol statutory and non-Europol statutory experts (irrespective of the event type Physical, Virtual, Hybrid); COVID-19 testing by external provider, etc.

The DPF continued working on the implementation of the transparency obligation to have the approved records of the processing activities published online in accordance with Article 31 (5) of Regulation 2018/1725. There are already 22 records of processing activities published online (https://www.europol.europa.eu/publications-events/publications/records-of-processing-activities).

5.2. Processing of Health Data

The establishment of the Europol Medical Service and the on-going consultations on its activities with regard to the processing of health data of Europol staff imposed additional challenges to the work of the DPF. As the processing of health data is a very specific processing activity requiring the adoption of additional data protection safeguards and the implementation of adequate technical and organisation measures in place, it is important to note that the DPF is not in the possession of specialised knowledge in this

[16] *https://edps.europa.eu/system/files/2022-02/22-02-28-remarks_at_jpsg_on_europol_en.pdf*

[17] 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

particular field and therefore can only provide advice to the data controller only to the best of its knowledge and abilities.

Since the beginning of the pandemic, the DPF took part in the Crisis Management Team and provided continuous support in the provision of privacy-oriented solutions to support the processing of related data at Europol. The DPF provided a continuous update to the CMT on novelties in the area of data protection compliance of COVID-19 measures. Particular difficulties were experienced due to the fact that Europol was one of the few EU agencies that kept presence in the office and hence, needed to face data protection related COVID-19 issues related to going back to work already in the first phase of the pandemic.

The DPF monitored closely the advice provided by the Dutch Health Authorities, the decisions taken by the government and the opinions issues by the Dutch Data Protection Authority. Specific advice was provided on the modification of the access control policy due to the implementation of the COVID-19 green pass for visitors; the processing of personal data in relation to the vaccination certificates; manual contact tracing, etc.

The DPF continued the provision of advice on transfers of medical files to Europol. On 16/06/21, the DPF launched a consultation with the EDPS with regard to the transfer to the Europol Medical Service. The EDPS reaffirmed the position of Europol with regard to the necessity of the transmission of the requested information to the Europol Medical Service. The EDPS requested formally assistance of the Dutch Data Protection Authority (according to Article 61 EUPDR) in order for Europol to obtain at least a copy the medical files from the previous provider of these services.

5.3. Prior consultation on proctored testing

In the beginning on 2021, the DPF was approached by HR for consultation concerning the data protection compliance of starting a proctored testing in the recruitment procedures. Test proctoring is testing overseen by an authorised, neutral, proctor who ensures the identity of the test taker and the integrity of the test taking environment.

With regard to the choice of the tool, Article 29 of Regulation 2018/1725 obliges the data controller (Europol) and processor (proctoring services) to enter into a data processing agreement, that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The agreement should also detail the controller's instructions with regard to data transfers (especially after the Schrems II Court Case), confidentiality and technical and organisational measures that are to be taken. It must be noted that the company providing the proctoring services also processes the data for its own purposes. In this context they are the data controller with respect to this processing of the data. Therefore, the DPF advised that the choice of the proctoring service should be very carefully made in order to ensure that a privacy compliant solution will be implemented.

In accordance with Article 39(1) of Regulation 2018/1725, 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'. The high risks to the rights and freedoms of natural persons are hence not only triggered by the processing of sensitive data but also from other elements, like the use of new technologies which are privacy invasive, as is in the case of proctored testing.

The data controller of the processing activities (Head of Human Resources Unit) drafted a record of processing activity, threshold assessment and a data protection impact assessment on proctored testing. In accordance with Article 40 (1) of Regulation 2018/1725 the controller shall consult the European Data Protection Supervisor prior to processing where a data protection impact assessment under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

The DPO advised the data controller taking into consideration that regardless of the implemented safeguards, security measures and mechanisms to mitigate the risk, the proctored examination can still result in a high risk to the rights and freedoms of natural persons, to launch a prior consultation process with the EDPS under Article 40 of Regulation 2018/1725 as the risks to the data subject rights cannot be sufficiently mitigated by reasonable means in view of the available technologies and costs of implementation.

In July 2021, the DPF launched a prior consultation with the EDPS on proctored testing. In August 2021, the EDPS requested additional questions which were answered by the data controller in cooperation with the DPF.

In October 2021, the EDPS issued an opinion on the prior consultation launched by Europol. Due to the similar issues at other European Union institutions and bodies, the EDPS requested agreement on publication of their opinion to which Europol did not object.[18] The data controller of the processing activity in cooperation with the DPF implemented the recommendations stemming from the EDPS Opinion and provided a documented evidence to the EDPS on 11/02/22. The EDPS was additionally informed that the data controller intends to commence the proctored testing unless advised differently by the EDPS.

5.4. Compliance activities regarding administrative data

Despite the limitations of on-the-spot compliance activities imposed by Covid-19 pandemic, regular compliance activities in the area of administrative data took place. The DPO issued a report on the compliance actions to assess the lawfulness of the processing of personal data in relation to the use of MIBO as a video chat promoted on IRIS for informal meetings and networking events of Europol staff (#1175392). In addition, on the basis of compliance activities in the area of security access to the Europol HQ, the DPO issued a Briefing note on the biometrical identification of staff and visitors (EDOC#1179198). Another compliance activities related to the special leave management at Europol on the basis of an inquiry in this particular area.

Regular meetings with contact points on administrative data processing took place ensuring that both sides keep each other informed about any novelties in relation to the processing of personal data.

The DPF continued the provision of advice to G2 on the data protection compliance of the transfers of personal data to a third country and in particular, whether the conditions laid down in Regulation 2018/1725 are complied with by the intended processor of personal data.

[18] https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check-and-prior-consultations/opinion-prior_en

The DPF was contacted by the Internal Investigation Service (IIS) on the conduct of two administrative inquiries. In the currently on-going internal legislation process on the adoption of a new legal framework establishing the IIS, it should be noted that the activities of IIS in general entail data protection risks for Europol due to the attached data protection responsibilities for the agency as a data controller. Europol as an agency stands out, as it acts outside of the arrangements of the Investigation and Disciplinary Office of the European Commission (IDOC, which is the body responsible for conducting administrative inquiries and disciplinary proceedings on behalf of the European Commission and among other EU institutions) where IDOC acts as a co-controller or processor and hence, have shared data protection responsibilities with the EU body in question.

Additional workload was also encountered in the handling of inquiries, complaints and advice on the handling of personal data breaches. Notably, the DPF conducted investigations on two inquiries launched under Article 13 of the DPO Implementing rules concerning the special leave requests and recruitment procedures. The DPF provided guidance to the data controller on 6 personal data breaches in the area of administrative data processing.

6. FINAL CONSIDERATIONS REGARDING THE ACTIVITIES IN 2021

Almost all activities of the DPO and his staff in 2021 required multi-disciplinary expertise and a holistic approach regarding the protection of personal data. In order to provide benefit to the controllers with regard to the quality and timelines of the guidance issued, to provide support during inspections or own assurance activities for fundamentally different processing activities, the DPF always considered both legal and technical-organisational aspects.

The close cooperation with all three departments and the continuous endeavour by the staff members working in the DPF to gain most updated expertise allowed the DPO to fulfil his tasks as foreseen by the Europol Regulation.

The activities in 2021 have been a prime example for the need to provide to Europol's dynamic processing environment continuous data protection support in form of consultation and coordination. At the same time to add value by providing to the controllers at Europol independent assessments on the compliance status of processing operations, which take place in a progressively sophisticated technical environment.