Speaking points

Role of EDPS

- The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. A number of specific duties of the EDPS are laid down in Regulation 2018/1725.
- The three main fields of work are
    - Supervisory tasks
    - Consultative tasks: to advise EU legislator on proposals for new legislation as well as on implementing measures. Technical advances, notably in the IT sector, with an impact on data protection are monitored.
    - Cooperative tasks: involving work in close collaboration with national data protection authorities (European Data Protection Board / EDPB which we also provide with secretariat)
- – monitoring and verifying compliance with Regulation (EU) 2018/1725 [GDPR for EU institutions, bodies and agencies],
    - giving advice to controllers,
    - advising the co-legislators on new legislation,
    - cooperating with Member States' DPAs,
    - handling complaints, conducting inspections
    - monitoring technological developments
    - Promoting data protection aware design and development

Main messages

- **Why care about data protection as border guards?** Data protection is about making sure that organisation handle information about people in a responsible way. We want agencies to collect what they really need (as public authorities: in order to fulfil the tasks assigned to you by law) and keeping it (securely, of course) only as long as it is necessary and being transparent about what you do and why you do it.

- There is a new legal framework for DP: Frontex applies Regulation 2018/1725, which is the sibling text to GDPR for the EU institutions and also includes a mini-LED. It is basically identical to those texts. It implies stronger focus on accountability and compliance requirements more closely linked to risks of the processing operations. The main principles, however, did not change.
- Over the last changes in the Frontex regulation, the agency has taken on a much more operational role; at the same time, operational cooperation between Member States has increased. As you all know from your own experience, when different actors conduct a common operation, everyone needs to know who is in charge of what and who is responsible for what. Data protection rules know this idea as 'joint controllership'. The new Frontex Regulation also explicitly mentions this possibility for some of the agency's activities (Art. 88).
- It means the idea of jointcontrollership (i.e. Frontex and MS involved) is implemented in practice. Controllers have to have an arrangement describing who does what, where this is not already defined by law. This is not a surprise: clearly defining who does what is key in any project or process involving multiple parties.
- For the EU institutions themselves, we have issued the Guidelines on concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 in November 2019, including what to cover in joint controller arrangements. The EDPB will soon do the same for the concepts of controller, processor and joint controllers under GDPR. Their content will be consistent, since the underlying concepts are the same.
- For practical steps: under the Frontex Regulation, the Management Board should adopt implementing rules on data protection. In preparing them, the assistance of Frontex' experienced DPO will be very valuable. The

DPO is also our main interlocutor at Frontex, and we keep in touch with

ETIAS (and controllership)

Overview ETIAS

Let's assess the issue using the example of the European Travel Information and Authorisation System (ETIAS) as established by the Regulation (EU) 2018/1240 (also known as the ETIAS Regulation) and aims at determining the eligibility of visa-exempted third country nationals prior to their travel to the Schengen Area, and whether such travel poses a security, illegal immigration or high epidemic risk.

- This Regulation (EU) 2018/1240 entered into force on 9 October 2018 and was adopted following two Communications of the Commission, which outlined the need for the Union to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism.
- In addition, ETIAS should support the Schengen Information System (SIS) objectives, namely by comparing relevant data from the online application files against the relevant alerts in SIS.

Therefore, ETIAS will consist of a large-scale information system composed by the **ETIAS Information System** (developed by eu-LISA), the **ETIAS Central Unit** (established within European Border and Coast Guard Agency - Frontex) and the **ETIAS National Units** (a competent authority designated in each Member State).

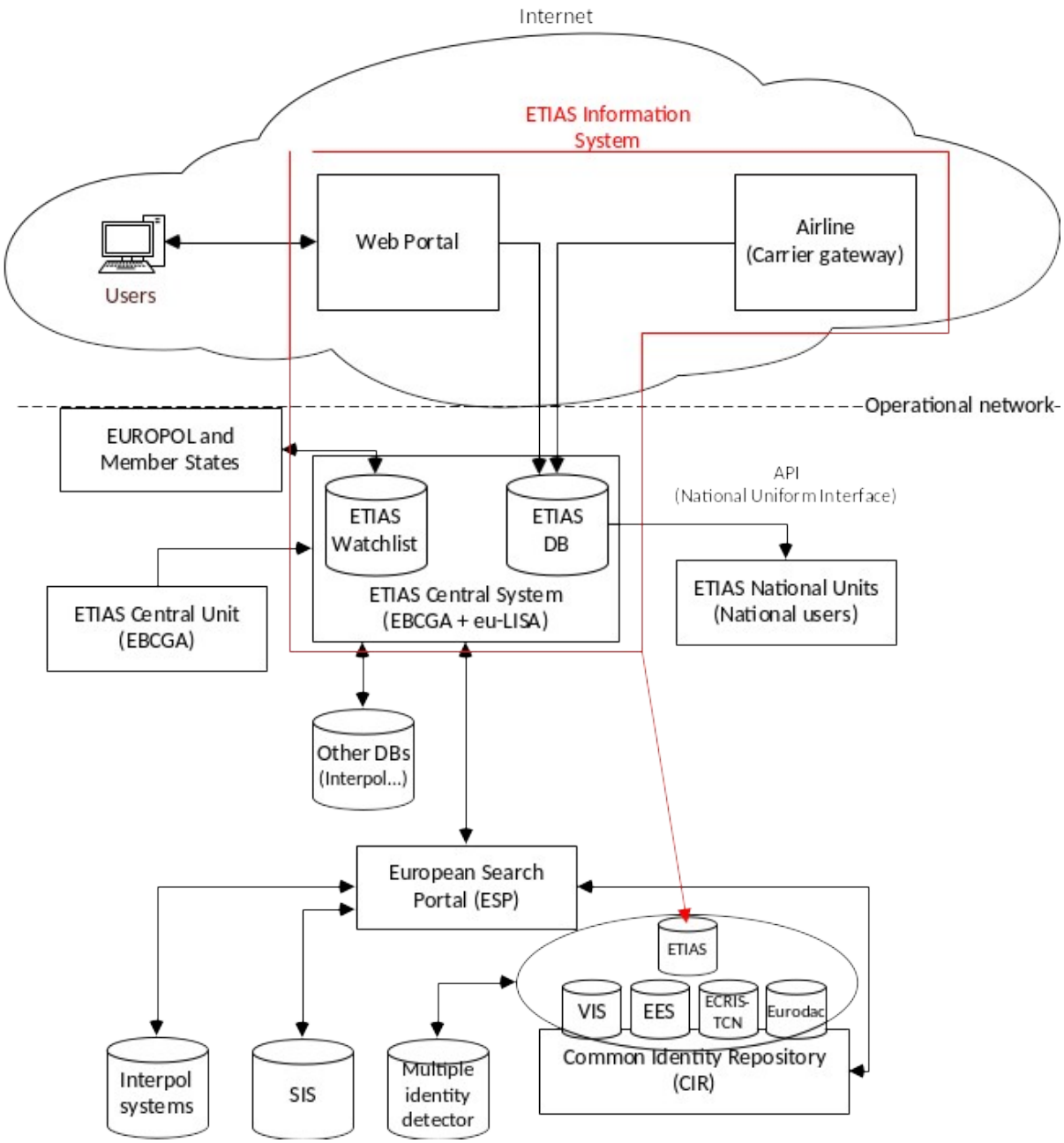
Frontex is the data controller in relation to the processing of personal data in the ETIAS Central System. Eu-LISA is the controller regarding the information security management of the ETIAS Central System and the processor regarding the processing of personal data in the ETIAS Information System.

The ETIAS National Unit is the controller for the processing of personal data in the large-scale information system – the ETIAS Central System – by a Member State.

The ETIAS Central System will examine each application file individually and compare relevant data with other databases to identify hits. For

example, it will automatically check whether an applicant is subject to a refusal of entry and stay alert entered in Schengen Information System, meets the specific risk indicators mentioned in Article 33 of the ETIAS Regulation or if the applicant is in the ETIAS watchlist.

Interoperability between the ETIAS Information System and other EU information systems (SIS, EES, VIS, Eurodac, etc.) and Europol data is therefore key.
In order to achieve its aim, the ETIAS Information System will be available for consultation of Europol, border authorities, immigration authorities and designated authorities of Member States.


Internet
ETIAS Information System
Web Portal
Airline (Carrier gateway)
Users
Operational network
EUROPOL and Member States
API (National Uniform Interface)
ETIAS Watchlist
ETIAS DB
ETIAS Central System (EBCGA + eu-LISA)
ETIAS Central Unit (EBCGA)
ETIAS National Units (National users)
Other DBs (Interpol...)
European Search Portal (ESP)
ETIAS
VIS
EES
ECRIS-TCN
Eurodac
Common Identity Repository (CIR)
Interpol systems
SIS
Multiple identity detector

What is the issue with controllership here?

- ETIAS is a complex system with many different players involved (see last page of this document); from the DP perspective, "controllership" is a functional concept: you look at who actually decides. In the ETIAS Regulation, some roles are explicitly assigned by law. However, that does not necessarily clarify things.
    - Example: Frontex is designated as controller for the ETIAS Central System, except for security, where it is eu-LISA [Art. 57(1)]. eu-LISA is also designated as processor for the wider ETIAS Information System [Art. 58], but it is not clear who the controller for the parts ETIAS that are not the central system would be. Additionally, eu-LISA has wider responsibilities during the development phase, including a requirement to follow 'privacy by design and by default' when doing so [Art. 73(3), fourth subparagraph, lit b].
- What does this mean for Frontex? As controller for the central system, they are for example responsible for ensuring data protection by design and by default. That means that they must play an active role in developing the requirements for the system. It also means that the obligation of making sure a DPIA gets done is on them [criteria: at least large-scale and special categories].
- Fuller explanation on ETIAS: ETIAS - Implementation - Strategy

Why is it our role to intervene here?

- ETIAS will be a highly visible system that will process personal data of millions of people and which will be used to support decisions made about them. For this reason, it is important that data protection by design and by default are properly implemented.
- At the same time, the complex setup with multiple actors involved presents risks of diluting responsibilities.
- For this reason, the EDPS has decided to follow the development of this system more closely.

EDPS practical actions about ETIAS

- General approach on how it will be built: ETIAS - Implementation - Strategy.
- EDPS opinion on proposal for European Travel Information and Authorisation System (ETIAS) (07/03/2017)
- EDPS took part in consultations on delegated acts (2019-0092 DG HOME - Draft Commission Delegated Decision on the ETIAS consent tool / 2019-0091 DG HOME - Draft Commission Delegated Decision on the ETIAS verification tool / 2019-0051 DG HOME - Draft Commission Delegated Decision on the ETIAS secure account service)
- Discussed controllership issue during visit to Frontex 26/09/2019,
- Meeting with Frontex and eu-LISA on 06/12/2019.:
    - data protection requirements to be more explicit in tendering documents, so contractors know what is expected;
    - Frontex and eu-LISA to clarify between them who is in charge of what exactly during the Data Protection by Design process
    - “Don’t use production data for testing”.
- This presentation
- High-level meeting with ED K.Garkhov (EU-LISA) confirmed in Strasbourg for 11 March 2020.