Position paper on the consultation: Consultation on the interoperability of EU information systems for borders and security

The following position paper states the opinion of the group on the proposed interoperability of security systems within the EU. Interoperability is understood as the ability of separately developed IT systems to exchange data and enable the end user to access this data. Furthermore, the data will be presented in a way it is understandable for the end user. The Commission assures the approach to be in full respect with the fundamental rights, data protection and with strict purpose limitations.[1] We highly appreciate the efforts that are taken to assure this.

Interoperability can improve the measures against identity theft, is able to reduce the risk of individuals being wrongfully arrested and can support the search of individuals who are reported missing. Although these improvements are beneficial for the general society we want to raise the Commissions awareness on the importance of **digital sovereignty and data security**, **quality of the data** in the systems and the importance to strictly limit **the access to the data.**

1.1 Digital Sovereignty and Data Security

The issue of digital sovereignty is not addressed adequately in the proposed solutions and strategy. The individuals to whom the collected data belong need to know what happens with their data. Otherwise it is not possible for the citizens in the European Union to form a fact-based opinion on the issue of interoperability. We wish the commission to follow their strategy on informing its citizens about the measures that are proposed. The commission is giving insides and little information on their information systems by handing out communication papers. An example is the paper from the 25.01.2017, which is informing citizens and third country nationals about which EU institutions are using the data that is collected.[2] At the same time it does not feature information with whom the data is shared once it is collected by national / EU officials and is fed into the databases SIS, VIS and EURODAC. In addition would be possible to mention the Decision (EU)

[1] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170629_interoperability_of_eu_information_systems_en.pdf Stand: 01.09.2017

[2] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20170125_eu_information_system_en.pdf Stand 01.09.2017

2016/920[3] which is giving the law enforcement agencies the authorisation to exchange of information for law enforcement purposes with cooperation partners in the United States of America. In a world where organised crime is not stopping at boarders and is often engaged in transnational acts of crime, an approach which is fostering security cooperation in the field of law enforcement is welcomed, but needs to be clearly communicated. This will give citizens the ability to gather knowledge on how and why data is being shared with other countries. As a benefit, it could restore the trust in data flows between third countries and the EU.

The recent decision of the ECJ regarding the agreement to share air passenger data with Canada shows how sensitive these data are and how important it is to follow privacy and data protection laws.[4] The proposed project must be aligned with the directive (EU) 2016/680 by Ensuring a consistent and high level of protection of the personal data of natural persons.[5] It is necessary to not only safeguard the personal data of EU inhabitants but also of third country nationals. The interoperability needs to be applicable with data minimisation and data consistency.

In the proposed solutions for interoperability there was no information in which ways the data is shared with third country actors. If the EU is cooperating with third country actors it should follow the principle of minimizing the data that is shared and set strict limits of legitimization. This is especially relevant in the area of asylum applications and is directly connected with the security of persons who pass the European boarders.

The proposed systems need to ensure that the database is protected against unlawful information sharing to the outside. Part of the data that is being processed in the system / systems proposed are visa entries, asylum application and data to identify individuals who are entering the European Union. These are sensitive information, which can be of great interest to criminal groups and foreign governments who are seeking to apply retaliatory measures. To grant full protection to individuals who are seeking international protection we must ensure that the collected data is not unlawfully shared with third countries, leaked to intelligence services or acquired by hackers linked to foreign governments or criminal groups. Following the argumentation of the FRA[6] the method used needs to clearly follow the protocol that is proposed for accessing the data. As Mr. Michael O'Flaherty

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016D0920

[4] https://www.reuters.com/article/us-eu-dataprotection-canada-ecj/top-eu-court-says-canada-air-passenger-data-deal-must-be-revised-idUSKBN1AB0T9

[5] DIRECTIVE (EU) 2016/680

[6] http://fra.europa.eu/en/speech/2017/fundamental-rights-and-interoperability-eu-information-systems

mentioned in his speech to the high-level expert group on information systems and interoperability these protocols weren't always systematically applied in the past.[7]

In order to fulfil its aspiration we advise the Commission to propose a system which applies the 'privacy by design' practice and is programmed to not display more data to the end user than necessary.

1.2 Quality of the Data

For an effective information system, the data quality is essential. As stated in the background paper to this consultation, interoperability can only work if the systems are fed with complete and accurate data.[8] We agree with this matter and want to highlight the importance of correct data to make fact based and correct decisions.

The FRA conducted a small-scale, representative survey, in which staff members at EU consulates where asked about the reliability of biometric data, visa and asylum request. Relying on this survey up to half of the staff members, which were interviewed in selected EU consulates, reported incidents of errant data or wrong matches in the system.[9] False or outdated data have a negative impact on visa or asylum decisions and can violate the fundamental rights of individuals.

To avoid this problem, interoperability needs to set certain standards and officials on the national level need to be able to use it in an adequate way. The data entries must be reviewed with certain quality standards. These process of data entries must be congruent. It does not simply solve the problem to open connection points between data bases or use a common platform for the data that is gathered within the member states or at its boarders. An example is the arrest warrant issued by the Republic of Turkey against the German citizen Dogan Akhanli.[10] The Republic of Turkey issued a red notice arrest warrant against Akhanli via Interpol. Which caused the arrest of the German writer with Turkish roots, by Spanish officials. Meanwhile the red notice was deleted. He was then later set free and the Spanish judiciary is proving its case. The request of extradition will be proved by the Spanish courts, but is unlikely to be carried out. The case now ended in the suspicion against Spain to support a politically motivated arrest warrant. The case was picked up by media institutions all over the world.

---

[7] http://fra.europa.eu/en/speech/2017/fundamental-rights-and-interoperability-eu-information-systems

[8] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170516_seventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

[9] http://fra.europa.eu/en/speech/2017/fundamental-rights-and-interoperability-eu-information-systems

[10] http://www.politico.eu/article/dogan-akhanli-spain-arrest-warning-to-turkish-dissidents/

This example shows how the outcome of a data entry, which later was deleted, can cause negative effects for individuals and on the same hand damages the image of law enforcement.
We propose an analysis tool which is fact checking and proving the reliability of the entries in combination with a training for national officials, which will work with the system.

1.3 Access to the data

In the *seventh progress report towards an effective and genuine security Union* the European Commission defines the key objective as giving border guards, law enforcement officers, immigration officials and judicial authorities the necessary access to information to protect external borders and enhance internal security.[11] Whilst the wish to simplify the access for these officials is understandable, systems like the two-step approach[12] lead to problems on the authorisation level.
We propose a request based system to avoid more access than granted.
A single search database or a two-step search could lead to discriminatory profiling, which causes a threat to fundamental rights. While risk assessment and profiling are common tactics of the border control, law enforcement and immigration officials, discriminatory profiling is an unjust practice. If an interoperable system displays sensitive data about race, religion or sexual orientation, there need to be certain safeguards implemented to avoid this practice.
If an official will have access to the names of persons that are in the different data bases, we face the issue of 'flagged hits'. This means, by constructing an interface in which the end user can search for a person and already knows the person is in a certain database without having the permission to access the files of the other database. The hit in the data base can already influence the decision of the official in a negative way. This is next to discriminatory profiling one of the biggest issues of a two-step solution or even a single search tool.

[11] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170516_seventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf
[12] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/20170726_background_consultation_interoperability_eu_information_systems.pdf