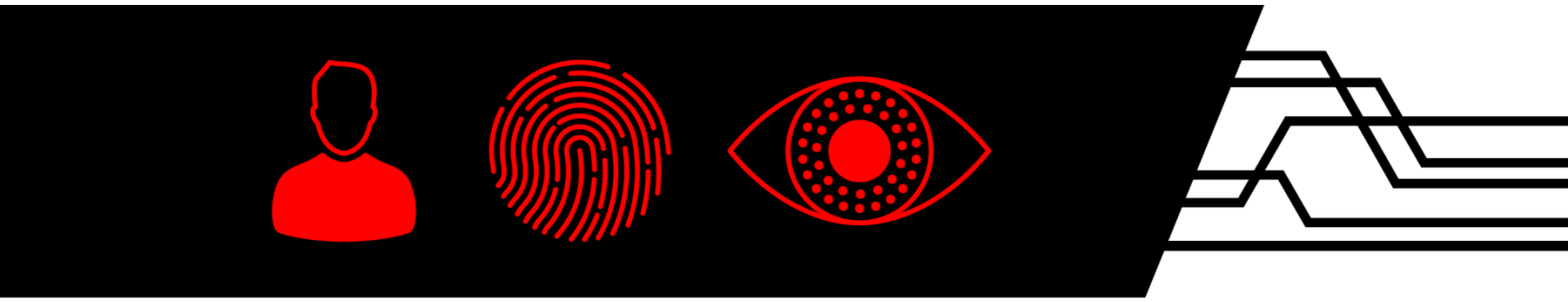

Biometric and Biographical Data-based Personal Identification and Identity Verification: Legal Regulations of European Union Member States

Research Report Summary

Tallinn, July-October 2016

The Research was ordered by the Estonian Ministry of the Interior within a RITA programme supported by the European Regional Development Fund that aims to increase the role of the state in the strategic managing of research and the capabilities of R&D institutions in carrying out socially relevant research. The project was funded by: European Regional Development Fund (50%) and the Ministry of the Interior (50%).

Link: **Research Report – Full Version (in Estonian)**

Authors:

Jekaterina Tšikova (Krabu Grupp LLC), an Identity Management and IT Expert.

Mari Pedak (Estonian e-Governance Academy Foundation), an Identity Management Expert and a Project Manager responsible for carrying out the research.

Helar Laasik (De Sapientia Partnerid LLC), an Identity Management Expert.

Katrin Nyman-Metcalf, PhD (Estonian e-Governance Academy Foundation), a Legal Expert; Public Information and Data Protection, incl. Identity Management Lawyer.

Research Report Summary

The purpose of this applied research was to attain an overview of the legal regulations across the European Union (EU) and Schengen Area member states in the field of biometric and biographical data-based personal identification and identity verification, and to determine whether the cross-usage of biographical and biometric data is enabled in various proceedings in the public and private sectors.

The research covered nine EU Member States – Estonia, Austria, Holland, Latvia, Portugal, Germany, Finland and the United Kingdom, and two parties to the Schengen Agreement – Norway and Switzerland. The research was based on two main data collection methods: (primarily internet) searches via publicly available information sources and interviews with identity domain experts. In addition to legal acts, important court cases were analysed and public discussion in the field was observed. Unfortunately, the interviews did not yield the expected input, because knowledgeable identity experts were very busy due to the actuality of their domain. This issue has been compensated through the search and analysis of additional data sources.

The study showed that the processing of non-sensitive biometric and biographical data in the public sector, including their cross-use in different public sector proceedings and transfer to private entities, is only permitted if the data are necessary in fulfilling legal obligations. The rules governing the processing of sensitive, including biometric personal data, are highly restrictive: the processing of biometric data in public sector proceedings is generally prohibited, except in cases where the processing is necessary to fulfil an obligation arising from law, such as the issuance of biometric identity documents. The purpose of data processing must always be clearly defined and personal data may only be processed for this defined purpose.

With regard to the private sector, the observed countries generally do not have separate regulations for biometric data collection and processing by private parties; the same laws are applicable to everyone. Basic rules are applied in such cases: since the data subject is the owner of his/her personal data, his/her consent is required for his/her data processing. Thus, data subject consent is the main (but not the only!) mechanism for justifying the processing of personal data in private sector relations.

The main focus in both the public and private sectors should be on the balance between privacy and security when processing personal data – the proportionality and necessity of data processing must be strictly examined. Even if the data are not used today, the collection of personal data might still violate someone's privacy.

Identity management is the area over which the EU has no control, and identity management rules differ from country to country. However, identity management strategies do not

recommend the creation of a unified or completely interoperable identity system. Rather, it is important to establish an adequate international technical interoperability that enables people to use secure cross-border electronic services and identity documents.

The EU is more active in regulating the electronic identity field than any other identity issue. EU regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) brings together a number of rules related to e-Identity and digital signature. This creates a common basis for secure electronic communication between citizens, businesses and public authorities, thereby increasing the efficiency of public and private sector internet-based services, e-Business and e-Commerce across the EU.

The EU's competence is greater in the data protection area, which is regulated by several directives and regulations, though individual member states have implemented details of these rules differently. This is one of the reasons why data protection in the EU is currently fragmented and uneven. The situation must change in 2018, when the new General Data Protection Regulation (GDPR) No. 2016/679 enters into force.

Estonia is a country with rather conservative but moderate data protection policies. Estonia provides an adequate level of data protection while leaving control over personal data in peoples' own hands and creating opportunities for the use of various public and private services.

As a result of the study, a number of recommendations and proposals for improving Estonia's identity management practices have been produced. The most important recommendations to be highlighted are the following:

- Estonia has extensive experience in the area of identity management and is a global leader in the context of e-Government. The authors of this Analysis Document, as well as many interviewed experts, recommend continuation of the current model that has been a key to the country's success, where:
    - identity management is performed by the state and in a centralised manner;
    - a person's identity is based on a personal code;
    - an identity card with electronic functionality is a compulsory national identity document;
    - a population registry is responsible for the management of a basic set of personal data, as well as for the quality and actuality of the population's personal data;
    - the identity schemes in use are based on reliable technologies (PKI) and allow people control over and responsibility for their identity.
- Travel Documents Assessment Centre should be restored in order to ensure strong identity management and help customer service representatives.
- Personal identification is not regulated by legislation in either Estonia or in the other studied countries, and the interpretation of terms varies significantly. The basic principles of personal identification should be regulated as a system of primary and secondary laws; both Personal Identification Best Practices and Identity Management

Glossary should be drafted for public and private sector institutions in order to avoid semantic confusions.

- The authorities involved into the issuance of identity documents should carry out self-evaluation (Identity Management Audit) according to the "ICAO guide for assessing security of handling and issuance of travel documents", ver. 4, 2016.
- The use of the biometric data template should always be preferred to the use of direct biometric data due to security reasons – the template requires less protection.
- Estonian identity management should be compatible with the environment being created by means of the EU's current Data Protection Reform. Dialogue on the proportionality is important when applying modern technological solutions that are necessary for secure identity management, on the one hand, and protecting people's privacy and avoiding the misuse of personal data, on the other hand.

The results of this research can be used in Estonian Identity Policy planning and implementation.

The Analysis Document is public and does not contain information that would require access restrictions to be imposed.