Andres Kivi

Compliance of the „once-only“ principle and General Data Protection Regulation in Estonia

Tutors: Laura Kask
Kaspar Kala

Tartu
2018
Table of Contents

Table of Contents ......................................................................................................................... 2
Introduction ................................................................................................................................. 4
1. “Once-Only” principle in legislation and policy documents ................................................. 5
   1.1. Once-Only Principle ........................................................................................................... 5
   1.2. Implementation of the once only principle in Estonian legislation .............................. 5
       1.2.1. Public Information Act ............................................................................................ 6
       1.2.2. General Part of the Economic Activities Code Act ................................................. 7
       1.2.3. Administrative Procedure Act .................................................................................. 8
       1.2.4. Government Regulation “Principles for Managing Services and Governing
              Information” ................................................................................................................ 9
       1.2.5. Draft proposal of the Personal Data Protection Act ................................................ 9
   1.3. OOP in policy documents of EU and Estonia ................................................................. 10
2. Compliance of OOP with GDPR principles ........................................................................... 12
   2.1. Principles of processing personal data and relation to GDPR ..................................... 12
   2.2. Lawfulness and transparency of processing .................................................................... 13
   2.3. Purpose limitation ........................................................................................................... 16
   2.4. Data minimization .......................................................................................................... 16
   2.5. Data accuracy .................................................................................................................. 18
   2.6. Storage limitation .......................................................................................................... 19
   2.7. Integrity and confidentiality ............................................................................................ 20
   2.8. Accountability ................................................................................................................. 20
3. Compliance of X-Road with GDPR ...................................................................................... 21
   3.1. X-Road and its components ............................................................................................ 21
   3.2. Compliance of X-Road with GDPR .............................................................................. 22
       3.2.1. Lawfulness and transparency ................................................................................... 24
3.2.2. Reuse of data (purpose limitation) ................................................................. 25
3.2.3. Integrity and confidentiality ........................................................................ 26
3.2.4. Data minimization ...................................................................................... 26
3.2.5. Data accuracy ............................................................................................ 27
3.2.6. Other principles of GDPR .......................................................................... 27
Conclusion ........................................................................................................... 29
References .......................................................................................................... 31
Introduction

The implementation of the “once-only” principle is a contributing factor towards creating an efficient Digital Single Market in the European Union. At the moment, when lots of administrative proceedings is done via paper documentation even in the oldest and most prosperous countries in Europe, truly employing “once-only” will result in two step advancement forwards. Countries, such as Estonia, who have embraced the core of “once-only”, have deemed the huge benefits of saving time and administrative costs by implementing the principle highly apparent, even for some experts to claim that cost-benefit analysis’ does not need to be conducted. In simplest words, the principle unburdens people, businesses and administrations from unnecessary interactions, when certain data was already supplied to any public administration before. The data is asked once and then reused. Until it is required by necessity.

According to the European Data Protection Supervisor, the “once-only” principle may raise questions in relation to major data protection principles stemming from GDPR. General Data Protection Regulation¹ or GDPR replaces the Data Protection Directive 95/46/EC and will be enforced from 25.05.2018. It was designed to harmonize data privacy laws across the European Union, to protect and empower data privacy of all EU citizen and to reshape the way organizations and persons approach data privacy.

This research paper was written within the IT Law Lab framework and the objective is to analyze the compliance of the “once-only” principle with the principles of GDPR in general and specifically in Estonia. In the first part, the author explores the implementation of the “once-only” principle in Estonian legislation, in the policy documents of the European Union and Estonia. Secondly, the compliance of the “once-only” principle with the principles of GDPR is analyzed and recommendations are made when implementing OOP cross-border. Finally, Estonian X-Road solution is investigated: the structure and compliance with GDPR is viewed through the prism of legal, technological and organizational aspects.

¹ Regulation (EC) No 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
1. “Once-Only” principle in legislation and policy documents

1.1. Once-Only Principle

There is no uniformly regulated legal definition of the “once-only” principle (OOP) in EU law. The article 9(2) of the Government of Republic of Estonia Regulation no 88 “Principles of Managing Services and Governing Information” from 25.05.2017\(^2\), stipulates that an authority shall not request a person to submit again the data that are required for providing a direct public service but are already in the database of the authority, or are included, as basic data, in any other database belonging to the state information system. Additionally, a person shall have an opportunity to inform the source of data about a change in the previously submitted data. Therefore, according to the regulation, the objectives of the once-only principle is to re-use the information already gathered from the citizens and supply it from one e-service to another in a secure and transparent way. The completion of these objectives will lead to elimination of administrative burden from both citizens and the governmental institutions in the longer time frame. Therefore, the components of once-only principle are:

1. ask data from the subject and never ask it again;
2. use and reuse the data asked.

1.2. Implementation of the once only principle in Estonian legislation

Estonian national system for data and information exchange among public administrations was selected as one of the best in the European Union.\(^3\) Therefore, the legislation in Estonia is an appropriate subject to inspect the implementation of OOP. Currently, Estonia is applying the OOP in the G2B, G2C and G2G areas.\(^4\) In similar fields, the principles of digital by default, common base registries, point of single contact, simplification of processes and legal requirements, reduction in reporting frequency, personalization of interaction, special help

---

\(^2\) Teenuste korraldamise ja teabehalduse alused. VVm 25.05.2017 nr 88. – RT I, 31.05.2017, 7.


\(^4\) Government-to-business, government-to-customer, government-to-government
functions and standardized semantics are implemented in the development and usage of ICT. The focus is set on functioning efficiently while interacting with data necessary for the provision of public services in a recognizable and systematic way. Government employs existing technological solutions and avoids duplicating by proceeding from the principle of reusability. The legislation enabling reusability is perpetually proposed and adopted. Through the principle of reusability, one half of OOP (reusability - see p 1.1) was already a systematic departure point of ICT development in Estonia. The other half (ask once) has found its way into legislation through the good will of the legislator in order to reduce administrative burden of its citizens.

1.2.1. Public Information Act

The purpose of the Public Information Act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties. Chapter 5 of the Public Information Act regulates databases, for instance the legal definition of a database, the state information system, determines the procedure for establishment of databases, names the chief (data controller) and authorised processors (data processor) of databases, coordinates the adoption of basic regulations for each database, names the definition of data types, database registration, access to databases and defines the support systems to state information system.

The § 43 of the Public Information Act states that the state information system consists of databases which are connected to the data exchange layer or X-Road and registered in Administration System for the State Information System or RIHA. It is allowed to establish a database by an Act or legislation issued on the basis thereof and prohibited to establish separate databases for the collection of same data. The existence of technical specification of each database in RIHA and legislation is intended to contribute in complying with the aforementioned prohibition. The § 43(2) of the same Act states the principle of reusability: the processing of data which are collected as basic data by another database belonging to the state information system (or connected to X-Road), shall be based on the basic data of the other database. The administrative authorities can compare existing databases and validate the need

for development of a new one. OOP is implemented via the aforementioned prohibition, the reusability clause along with the precise regulation on establishment and management of information systems and the legal grounds for basic data reusability.

For example, E-File System, which is a information system for processing of procedural and personal data in the course of civil, criminal, misdemeanor court proceedings, is legally based on the Statute of E-File System. The data sets entered into the E-File System are stated in the procedural acts, such as Code of Civil Procedure, Code of Criminal Procedure and Code of Misdemeanor Procedure. The data controller of the E-File System is the Ministry of Justice. If a person wants to know, which types of data is entered to the database, he should familiarize himself with the RIHA entry on E-File System and the legislation behind the information system. If a governmental agency is assigned a new task, the completion of which is dependant on gathering personal data, the first step is to query RIHA, if the data is already used as basic data of another database. If the answer is positive, then the developing e-service would have to be linked with the database. If the answer is negative, then new legislation and creation of a database would have to be forced. Through documentation, verification and legislation of databases, e-services and information systems, the symptom of data duplication is reduced or completely abrogated.

1.2.2. General Part of the Economic Activities Code Act

The General Part of the Economic Activities Code Act was passed on 23.02.2011 in order to establish general conditions of and procedure for exercising the freedom of economic activity, including to regulate the commencement, pursuit, termination and resumption of economic activities, the maintenance of a register, state supervision and liability, according to § 1 of the Act. The implementation of OOP is referenced in its § 13.

General Part of the Economic Activities Code Act § 13 states, that it is prohibited for economic administrative authorities to require from undertakings and undertakings need not submit information which is entered in a database established pursuant to law, except for information which allows the identification of an undertaking and contact details of an undertaking.

7 Algtekst. Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seadus 1027 SE. Available at: https://www.riigikogu.ee/tegevus/eelnoun/eelnoun/1cb8151b-c5d2-3f1b-8665-489d7ac1c56b/Avaliku%20teabe%20seaduse%20ja%20sellega%20seonduvate%20seaduste%20muutmise%20seadus
Additionally, according to § 13, the prohibition on requiring information twice also applies to information which can be obtained free of charge from the relevant register of another Contracting State or for a charge if the undertaking confirms in a format which can be reproduced in writing that it covers such costs for obtaining the information. The prohibition on requiring information twice does not apply to the information in the registers of third countries.

The explanatory memorandum\(^9\) of the aforementioned act states that any kind of action considering asking data that has already been requested before and recorded in any governmental register by an administrative authority is forbidden. Hence, the administrative authority is obligated to take into consideration the data previously entered into the registers. However, the prohibition on requiring information twice is not applicable to the cases where information which allows the identification of an undertaking and contact details of an undertaking is requested. Thus, on certain occasions, the breach of OOP is allowed.

1.2.3. Administrative Procedure Act

One of the most important principles of Estonian administrative procedure is the principle of investigation, which is regulated in the § 6 of the Administrative Procedure Act\(^10\). According to it, during proceedings in a matter, an administrative authority is required to establish facts relevant to the matter and, if necessary, collect evidence on its own initiative for such purpose. The act does not specify, to which extent the principle of investigation is implemented. Via other provisions of the act, it can be concluded, that gathering evidence and investigating the factual background has to be easy and effective. Likewise, the collection of data has to be appropriate, necessary and purposeful.\(^11\) Accordingly, it means that during administrative investigating process, the investigator has to access various databases on his own and not trouble the person with data requests on some data already entered into a database connected to X-Road, because doing so would mean the breach of the proportionality and investigation principles.

---

\(^9\) Majandustegevuse seadustiku üldosa seletuskiri. SE 806. Available at: [https://m.rigikogu.ee/tegevus/eelnoud/eelnou/ea277f5e-517d-e7d4-0-0274-b1b8247c5de5/](https://m.rigikogu.ee/tegevus/eelnoud/eelnou/ea277f5e-517d-e7d4-0-0274-b1b8247c5de5/)


As one of ways for the beginning and end of term of administrative proceedings is the proceeding on the initiative of the administrative authority (§ 33(5)). This proactive way of administration leads to decrease in administrative burden from the citizens, since administrative authorities begin the proceedings on the data entered into state information system and the data subject does not have to apply for it. For example, a child is given illness insurance directly after birth, based on the data inserted to another database.

Additionally, the Administrative Procedure Act § 7(4) states that in administrative procedure the rules and requirements for processing personal data shall be observed pursuant to the Personal Data Protection Act. The reference to Estonian data protection act denotes the importance of data protection principles in the administrative procedure. Through EU legislation supremacy principle, direct applicability of GDPR and adoption of its principles, the exposure of GDPR principles towards Estonian administrative procedure is constituted.

1.2.4. Government Regulation “Principles for Managing Services and Governing Information”

Government Regulation No 88 “Principles for Managing Services and Governing Information” of 25.05.2017 establishes as the principles for managing services and governing information, the requirements for management and development of services and information governance. It’s § 14(2) states, that authorities shall cooperate to share information and use it for the provision of the services. The regulation establishes the management and development of services and information governance as digital-by-default. The § 2(3) also regulates the definition of proactive services, which are the direct public services provided by an authority on its own initiative in accordance with the presumed will of persons and based on the data in the databases belonging to the state information system. Thus, with proactive services, the data from state information systems is reused, reducing the administrative burden of the citizen.

1.2.5. Draft proposal of the Personal Data Protection Act

GDPR has forced the Estonian legislator to adopt a new Personal Data Protection Act, which should comply better with the GDPR. Draft proposal of the legal act\textsuperscript{12} was prepared by the Justice Ministry of Estonia. The secondary processing of data or data reusability is currently

regulated stricter, than in the GDPR. The legislator has opted for a closed catalogue of bases for legalization of secondary processing\textsuperscript{13}. Draft proposal § 6(1) states, that administrative authority may process data on any other purposes, other than on which data was firstly gathered, only if its necessary on the grounds of public security, prevention of offenses or to protect the obvious interests of the data subject and is allowed by law. Contrastingly, article 6(4) of the GDPR gives a set of proportionality rules, which can be used on any legal grounds, when proportionality is observed with considering the rights of the data subject and the public interests.

The § 6(1) of the draft in this wording is detrimental to the promotion of data exchange. Further processing is extremely restricted, since a closed catalogue of legal bases is proposed, which allows further processing of data only for certain purposes needed for law enforcement agencies. However, the explanatory memorandum of the draft proposal specifies on multiple occasions as one of the objectives the “continuing triumph of the e-state” and admits the importance of cross-usage of data as one of the components of it. Although it might be dubious, it might be concluded, that the authors of the draft proposal do not consider the exchange of data via X-Road as data processing. Since X-Road is a secure platform for data exchange and it’s only accessible to the participants of the system and in itself, the organization administrating X-Road is not a controller nor can access the data exchanged via the layer and only grants admittance to new members of the X-Road, the data exchange in this layer is not data processing in the classical sense.

Consequently, two solutions are at hand, pursuant to determining whether the exchange of data in X-Road is considered as processing of personal data. Either the legal base for further processing is settled or the exchange is \textit{expressis verbis} constituted not to be processing of personal data in the Act itself or the explanatory memorandum.

1.3. OOP in policy documents of EU and Estonia

Both the European Union and Estonia have developed policy documents on the exploitation and development of ICT’s in the area/country, which provide the details of either Member States’ or governments commitments in relation to what needs to be done in order to achieve

objectives set. Policy documents serve as implementation plans or guides for development of ICT.

Creating a Digital Single Market was presented as one of the political guidelines of the Candidate for President of the European Commission Jean-Claude Juncker on 15.06.2014. In order to achieve this, the presidential candidate vowed to take ambitious legislative steps towards a connected Digital Single Market. As a staple of non-legislative work, the “EU eGovernment Action Plan 2016-2020” was presented, which referred to the OOP as an underlying principle of the development of eGovernment in European Union. This document targets three areas to improve electronic governance in Europe from 2016 to 2020: modernizing the public administration, achieving a digital internal market and engaging more with citizens and businesses to deliver high quality services. European Commission supports the implementation of the once-only principle, because it decreases administrative burden by ensuring that citizens and businesses supply certain standard information only once, assuming that public administration offices take steps internally to share the once requested data, so that no additional data queries have to be made by the authorities.

Additionally, public administration offices take action if permitted to internally re-use this data, in due respect of the data protection rules, so that no additional burden falls on citizens and businesses. Thus, the action plan clearly presents the hierarchical superiority of data protection principles over OOP. The Tallinn Declaration on eGovernment of October 2017 has set an objective of achieving the purposes of the once-only principle by 2022, as 24 legislative initiatives have already been presented and 6 initiatives have been completed by the European Commission.

Lots of administrative actions are duplicated, mirroring the low efficiency from the paper documentation era, an Estonian action plan has found in 2015. “Digital Agenda 2020 for

---

16 Ibid.
Estonia”\(^{20}\), a policy document issued by the Ministry of Economic Affairs and Communications names as one of the principles of the development of information society in Estonia the organization of the public sector processes so as to ensure that citizens, entrepreneurs and public bodies will have to provide any information only once. As one of the action lines in order to improve the quality of public services through harmonization and cooperation between public bodies is the development of processes behind the provision of public services and the supporting ICT solutions to ensure the once-only submission of data.

2. Compliance of OOP with GDPR principles

Success of Estonia, Netherlands and Belgium and others\(^{21}\) reusing data, namely the cost-effectiveness, reduction of administrative burden and other positive impacts have galvanized the efforts to implement OOP on the European level. Basically, specified base data requested by any governmental agency or institution in Europe, which is entered into any linked database will have to be reused by any governmental institution in every other country in Europe, while complying with the principles of GDPR. An analysis of GDPR principles in context of implementing the “once-only” principle is produced below.

2.1. Principles of processing personal data and relation to GDPR

Article 5 of the GDPR names that personal data has to be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in


accordance with Article 89(1), not be considered to be incompatible with the initial purposes
(‘purpose limitation’);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they
are processed (‘data minimization’);
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure
that personal data that are inaccurate, having regard to the purposes for which they are
processed, are erased or rectified without delay (‘accuracy’);
(e) kept in a form which permits identification of data subjects for no longer than is necessary
for the purposes for which the personal data are processed; personal data may be stored for
longer periods insofar as the personal data will be processed solely for archiving purposes in
the public interest, scientific or historical research purposes or statistical purposes in accordance
with Article 89(1) subject to implementation of the appropriate technical and organizational
measures required by this Regulation in order to safeguard the rights and freedoms of the data
subject (‘storage limitation’);
(f) processed in a manner that ensures appropriate security of the personal data, including
protection against unauthorized or unlawful processing and against accidental loss, destruction
or damage, using appropriate technical or organizational measures (‘integrity and
confidentiality’).

The European Data Protection Supervisor has stated\textsuperscript{22} that in order to ensure successful
implementation of the “once-only” principle in the European Union and enable lawful cross-
border exchange of data, the principle has to be implemented fully in line with relevant data
protection principles. Therefore, the compatibility of OOP and GDPR principles is analyzed
below.

2.2. Lawfulness and transparency of processing

Article 5(1)(a) of the GDPR sets “lawfulness” as a principle of data processing. It means, that
data controllers or processors must have legitimate grounds for collecting and processing
personal data in order to become “lawful”. The “lawfulness” of processing personal data is
further explored in the Art 6 of the GDPR via establishing different legal bases for lawful

\textsuperscript{22} Opinion 8/2017. EDPS Opinion on the proposal for a Regulation establishing a single digital gateway and the
processing, which are the data subject’s consent, necessity stemming from contractual obligations, necessity deriving from an obligation set by law, necessity emanating from protecting the vital interests of a natural person, necessity coming from the performance of a task carried out in the public interest or necessity arisen due to pursuing legitimate interests of the controller or third party. The most relevant legal grounds for implementing the OOP are consent (article 6(1)(a) of the GDPR), legal obligation (article 6(1)(c) of the GDPR) and performance of a task in public interest (article 6(1)(e) of the GDPR). 23

The legal ground of consent gives the most control to the data subject - he can decide, whether to make data processing legal. 24 The main condition for a valid consent is that it has to be freely given by the data subject. The difficulty of consent lies within the imbalance of the sides: government provides e-services, which make a lot of actions between the citizen and the government easier and faster - therefore, the data subject may be forced to give consent on specific data, because he wants to access some services, even if the requested data would not be needed for reaching a certain purpose. For example, the regulation on the tax marks’ database has to specify, which data can be inserted into the database and exclude the possibility that information on data subject’s health be entered by coercing the consent of the data subject. Therefore, to poise the legal relationship between the data subject and the controller, legal boundaries of consent have to be stipulated.

In the context of OOP, the legal base of consent gives the data subject discretion to decide, if he allows the processing of data. However, it might be hard for the data subject to comprehend why should he allow the recurrent processing of data to different countries and institutions. Additionally, consent can be withdrawn, therefore, initiating a procedure of data deletion, which is in itself an increase in administrative burden.

Another legal basis for personal data processing is a legal obligation of a data processor. 26 It is the least flexible legal ground for data processing, because the legal obligation must also


determine the controller, type of data processed, specifications of determining the controller, purposes of processing, entities to which data may be disclosed, purpose limitations, storage period and other measures to ensure lawful and fair processing. This basis may be used by entities where the obligation to process personal data is enforced by law. It may only be used in cases where law unequivocally demands performance, not just permits it. Although the legal basis is very strict in implementation, the strictness creates the most legal certainty, because data subjects know which data is processed under which conditions and can exercise his rights in the easiest way.

The third relevant legal ground for processing personal data in the context of OOP is the public task or exercise of official authority. The public task or exercise of official authority is given by law, therefore, this legal basis is similar to the one described previously: legal ground has to be present, therefore same reasoning applies to this legal base also.

The best solution to settle problems is to prevent them. The bases of legal obligation and the performance of public task or exercise of official authority allow legal clarity from the beginning of processing. The specifications of processing, such as the controlling and processing entities, the type of data used in processing and other information, is stated in the governing acts of the information systems. The dependency on the data subject is decreased, since he cannot withdraw the consent or decide on the lawfulness of data collection and reusability in each separate case. Consequently, the best legal bases in the context of OOP are legal obligation and performance of public task or exercise of official authority.

The transparency principle in the context of OOP is the reuse of data by the public sector in a clear and straightforward way, which is accompanied by a transparency mechanism where the user could see what data is accessed by which government office for which purpose. This principle aims to create trust between the government, citizens and businesses. Transparency is achieved via user logs, notifications of data requests and a person’s correct expectation of data processing. Additionally, to achieve transparency through technical measures, a registry

---

27 Recital 45 of the GDPR: „Where processing is carried out in accordance with a legal obligation. including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association. “


of databases has to be created, which has to include information about which data is stored in which database (European level analogue of RIHA). Data types in each database have to be flagged in a machine-readable universal language, so that data can be accessed by different information systems.

2.3. Purpose limitation

The principle of purpose limitation regulated in the Article 5(1)(b) of the GDPR. The purpose limitation principle is observed when the processing of personal data is permissible if and to the extent that it is compliant with the original purpose for which data was amassed and as far as the data controller can exhibit the data subject has consented to use the data for aforementioned purposes. In consent cases, it is illegal to process data collected for a specific purpose for any other purpose. In case the data controller wants to operate the data for other purposes, it has to ask for another consent for the new purposes. Exceptions can only be made on the grounds of national security, national defence, fight against crime and other objectives of general public interest of the same level listed in Art 23(1) of GDPR.

On other legal bases than consent, the further processing is allowed, if the further processing is based on law or meets the criteria stipulated in Art 6(4) of the GDPR. The factors of link between initial and further purposes, context of collection, nature of the data, the possible consequences for the individuals and safeguards have to assessed in order to verify the compatibility with Art 6(4). The danger of implementing of OOP lies in the assumption that OOP is always employed in public interests and compatibility rules do not have to be followed. The assumption is wrong, however, as reducing administrative burden is not a valid ground for restricting GDPR effects under art 23(1). Therefore, administrations should regulate the secondary processing in laws and statutes, which have to be clear and determine which types of data and by whom may be processed on which occasions.

2.4. Data minimization

Data minimization is referenced as a principle in article 5(1)(c) of the GDPR. The principle means that data controllers and processors have to ensure that they collect and process personal
data which is necessary for a specific purpose, also considering the length and place of data storage. Consequently, the data controllers should only collect the personal data they really need and should store it only for as long as they need it in a predefined storage location. Therefore, the compliance of OOP and data minimization principle is ensued from three factors: the subject matter of data collected (“which data is essential to be collected”, the physical and virtual locations of data (“where the data is stored both physically and virtually”) and the time length of data storage (“which time is essential to re-use data while offering e-services”). The third aspect or the length of data storage is addressed as the storage limitation principle below.

Nowadays, unnecessary data is still collected in some European countries. The data in those cases is unnecessary, either because the world has moved on (e.g. name, address, phone number, when a unique identifier can be attached) or the requested data is assumed to be useful for some other undefined or unknown purpose (e.g. data mining or analytical purpose)\[30]. The specification of base data is the core of data minimization – it should be predefined, which data is necessary in order to fulfill obligations stemming from law and public interests. Should base data not be defined, the principle of data minimization cannot be achieved, since unnecessary data would be collected.

The physical and virtual storage place of data is also a component of the OOP, since data is stored in only one location, instead of many different locations. Therefore, after implementing OOP, a data repository in Italy containing personal data of an Italian citizen would be accessed by an Estonian, if the Italian citizen decided to live for Estonia and other countries for few years each. Basic data, physically and virtually stored in Italy and Italian database of this citizen would first be used by Estonian authorities then shall be re-used all over Europe, minimizing the amount of same data, which would be collected all over again in different countries. This is one of the biggest advantages of OOP implementation in the context of GDPR.

Therefore, the solution is to define the base personal data which is enquired by the controller. The recognition of some data to become non-basic, such as name, address, race, phone number, e-mail address and only establish a personal identification code as a sole personal data subject matter would ensure that the minimization principle in this aspect is satisfied to its fullest.

Hence, whenever an identification code is sufficient to enable a successful provision of a service, no other data has to be asked by the controller.

Technically, the designation of the location the data storage location is essential to minimize the amount of duplicated data in different information systems. The designation of the storage location should be determined either by the citizenship or residency of the data subject, the origin of personal data, characteristic data type (e.g. all medical data in a central database or all sensitive data separately) or other possible factors. The determination has to be in compliance with the technical solution of OOP implementation, for example, it would be counterproductive to

In order to promote data minimization on EU level, a codified list of data types would have to be applied, which would stipulate, which data types may be used for cross-border data exchange in which cases. Even more importantly, the physical and virtual storage of data must either be designated according to the origin country of data, citizenship, residency or other factors. The minimization of matter and the limitation of storage place to one location only would enable the implementation of OOP on a European level.

2.5. Data accuracy

Article 5(1)(d) of the GDPR enacts the principle of data accuracy, which ensures that personal data collected during data processing is accurate. Provided the collected data is inaccurate, the processor has to take all possible actions to amend the collected data. Should the rectification of data be impossible, then the affected data has to be anonymized or deleted without delay. It is impossible to comply with the data accuracy principle in full, since lots of data in the databases might be subjective, such as diagnoses of medical doctors or false data may be presented by the data subject on purpose or entered incorrectly due to human error. Since a certain medical diagnosis may lead to a pension from the State and this data would be enquired from the same database, the inaccurate data may lead to completely different legal outcomes.

In order to promote data accuracy in the European-wide OOP context, the unification of databases in different countries and languages has to be created, which would map all data using metatext and be able to translate it accurately and correspondingly, using a predefined catalogue
of words. Translated and pre-translated data has to be made available to the subject, in case there is false data or the subject understand the original data entry.

The correction of false data has to be based on the activity of the data subject, therefore, an option to request an amendment of data has to be ever present and technically enabled by the data exchange solution. This means, that if an Estonian data subject requests data from the Estonian e-service and Italian database has false data on the subject, the subject has to have a technically easy solution to report the data and possibly to insert corrected one, which is achieved via the technical solution of the information system (activity of the controller) and the support of the data exchange system (passive ability of the processor).

2.6. Storage limitation

Storage limitation principle is noted in art 5(1)(e) of the GDPR. Data controllers or processors can only store personal data in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In context of OOP, it is unknown, for how long certain data may be necessary for storage. Therefore, the difficulty lies within predicting which data may be necessary in the future on another purpose.

The limitation has to be set in time length and has to be dependent on types of data. For example, certain health and biometric data will never change, such as race, sex, eye color, fingerprints or hereditary illnesses.

While storing data on the subject’s race, sex and eye color may be justified for a period of data subject’s life, the data on fingerprints or hereditary illnesses may prove useful in the future. Data on hereditary maladies can be very useful, in relation to both an individuals or general public’s interests. The storage limitation is set by the data controller, but during the implementation of data exchange, it has to be considered to harmonize the storage limitation in different European countries, e.g. data on hereditary diseases has to be stored for 300 years in all countries of the EU. The storage limitation can be enforced through a unified exchange layer, for example, if a certain type of data was once entered into a linked database, it won’t be deleted for a predefined amount of time.
2.7. Integrity and confidentiality

The integrity and confidentiality principles mean that data controllers and processors should analyze, whether only authorized users have access to data by using strong passwords, two step identification and identification methods with high levels of assurance, such as ID-card or m-ID in Estonia, enable the automatic log-out after certain amount of inactivity etc. The integrity and confidentiality is closely tied to eIDAS regulation\(^{31}\) and is key to building trust in the online environment and governmental e-services.

In order to establish a secure implementation of OOP, the data protection would have to be ensured by design and by default specified in article 25 of the GDPR. The article proposes the technical solution of pseudonymisation as one of measures for it.

Additionally, when implementing OOP, one should consider that access to data is restricted to only those authorities and services, which definitely need the data. As one of the solutions, the accountability of the controlling entity may be useful: data controller itself decides, whom the access is granted, after the request to use the database was given by the applicant. Therefore, even if one database or information system is attacked or breached, other information systems will remain secure.

Should the personal data processing and storing be organized and managed by one agency centrally, higher thresholds of verification and security have to be instilled. In this case, a data leak or system breach of the technical solution would probably allow to access, modify and otherwise use data to unauthorized persons.

2.8. Accountability

Art 5(2) of the GDPR specifies the principle of accountability. Data controllers should demonstrate that while processing data they are also complying with the GDPR principles and also state their responsibility for complying with them. Measures taken in order to comply are appropriate in relation on the nature, scope, context and purposes of the relevant processing and also take into account the risks and freedoms of data subjects.

The accountability stems from the person of the data controller. Depending on the organizational solution behind implementing OOP, the accountability may become an issue. If all the data would be stored, managed and organized by the same governmental agency, it would become too powerful and breach the principle of dispensed power in democracy. Therefore, a single data repository and controlling entity may become an issue, since it’s less secure, stable and must have much more competences to be effective. If the data would not be controlled by a centralized repository, such as in case of Estonian X-Road, the accountability would have to be shown by the agencies using the system, not the organization maintaining the technical uptime of the information channel.

3. Compliance of X-Road with GDPR

3.1. X-Road and its components

X-Road is the backbone of e-Estonia. It was commenced by the Estonian government in the 1990’s and started operating on 01.01.2001 to construct a secure and standardized infrastructure for the interoperability of governmental registries, without compromising security of the data with the capability of organic integration with existing and new systems. The secure data exchange layer of X-Road, creation of unique personal and company commercial identification codes, which provide the opportunity to merge data from different registers and RIHA catalogue together support the establishment of e-Estonia. E-services, such as citizen portal, Estonian e-health system, e-prescription system, e-file system and e-police system were enabled to be created, which was one of the main factors to contribute in order to push Estonia into the digital innovator status of today. The most queried X-Road

---

32 X-Road. Available at: https://e-estonia.com/solutions/interoperability-services/x-road/
34 X-Road. Available at: https://cyber.ee/en/e-government/x-road/
35 Estonian data exchange layer for information systems (X-Road), 2017. Available at: https://scoop4c.eu/cases/estonian-data-exchange-layer-information-systems-x-road
services are the Register of taxable persons, Estonian Medical Prescription Center, Health Insurance Information System, Land Register and Estonian Register of Buildings. 37

Public and private sector enterprises and institutions can connect their information systems with X-Road. 38 The membership of X-Road is available to legal persons that meet the requirements specified in § 15-20 of Regulation No 105 of the Government of the Republic of 23.09.2016 “Data exchange layer for information systems”. According to article 4 of the regulation, the Information System Authority or RIA develops and administers X-Road, but does not have access to data stored in linked information systems. Therefore, the core of OOP is hard-wired into the base of X-Road architecture, since clear ownership rules around personal data and the availability and reusability of this data to other institutions is established.

From a technical viewpoint, the system is fundamentally a peer-to-peer system with interoperability being enforced by centrally distributed software rather than standards. It employs a versatile security solution via authentication, multilevel authorization, high-level log processing system, encrypted and time-stamped data traffic 39. All in all, X-Road consists of four parts: technical, organizational, semantic and legal, none of which is capable of delivering full value apart from others. 40

3.2. Compliance of X-Road with GDPR

The article 4 of the GDPR determines the definition of data processing as any operation or set of operations, which is performed on personal data or on sets of personal data, followed by an open-catalogue of examples. Additionally, the definition of data processing in computer science is as following: “Manipulation of data by a computer... Any use of computers to perform defined operations on data can be included under data processing.” 41 Therefore, the definition of (personal) data processing is very broad and means virtually any exposure of personal data to computers. Thus, even the data exchange through X-Road is data processing in the GDPR sense and has to be compliant with the provisions embodied within it.

37 X-Road. Factsheet. Available at: https://www.ria.ee/x-tee/fact/#eng
The role of X-Road or RIA, the institution which manages and develops it, is debatable in the context of GDPR. Firstly, it certainly does not respond to the definition of a controlling entity, since it does not determine the purposes and means of processing personal data. Secondly, X-Road is not a legal person, therefore cannot be specified as a controller, but RIA is. Although RIA does not determine the purposes of data processing, it maintains the information channel, which allows further processing in form of data exchange. The exchange of personal data between different information systems is a base of the Estonian eGovernment. Through the broad definition of “processing”, enabling the exchange of personal data between various actors through X-Road has to be defined as falling under the scope of this definition. In order to complete the exchange of data, the controller and data subject must sign a contract enabling it. The technical solution of X-Road is used to complete the exchange. Therefore, one of the objectives of processing personal data, the reusability, is achieved via X-Road. Due to every institution in Estonia processing personal data also having the objective to exchange it via X-Road, the institution managing X-Road or RIA, might fall under the definition of “data processor” of the GDPR, since it is enabling personal data exchange on the behalf of various data controllers. Nevertheless, defining RIA as a processor in all cases of data exchange might seem rigid, since this authority does not actually control the content of the messages transmitted, merely sustaining the system technically and granting access to use it. Interestingly, the role of RIA as a processor isn’t apparent in the Estonian regulations – in fact, it is never specified as one. Although specifying the processors isn’t mandatory, RIA has an important function of enabling data exchange between entities, which is a type of data processing, making RIA a data processor.

Interoperability of databases is the core feature of the Estonian eGovernment system, which is achieved via a layer of data exchange. As stated previously, X-Road is comprised of technical, organizational, semantic and legal components. This research paper will analyze the compliance of X-Road with GDPR from legal and some technical and organizational aspects.

---

3.2.1. Lawfulness and transparency

The legal ground for first-time data processing is given by law to exercise official authority or complete a public task. For example, the Health Information System is processing personal data, so that the Ministry of Social Affairs could fulfill the obligation of protecting public health, enabling better quality medical services and the assurance of patients’ rights.

The transparency of processing is achieved through the adoption of information systems’ base regulations, which stipulate the identity of the controller, the purposes of processing and further information on processing. For example, the transparency of initial processing of health data in the Health Information System is assured in the relevant Statute as it specifies the Ministry of Social Affairs of Estonia as the data controller and imposes the objectives for processing personal data as a necessity to provide and improve healthcare services, secure the rights of citizens and others. Therefore, the initial processing via X-Road is both lawful and transparent.

As for the lawfulness and transparency of secondary processing, there exists a significant legal problem due to imprecise wordings, such as “for the completion of its tasks, a database may exchange data with other databases via X-Road.” This imprecise wording breaches both the lawfulness and transparency principles, since it isn’t clear and easy to understand, which persons will use specific data for further processing. In order to comply with lawfulness and transparency principles, it is essential to regulate who has access to process the data on which grounds, purposes and other terms stemming from GDPR. In Estonian case, the § 43(1) of the Public Information Act rectifies that composition of data of a certain database and the persons submitting data to it is regulated by the statute of the information system. Essentially, this means that all types of data and the data submitting entities have to be named in the statute. For example, the further processing of data in the Health Information System is regulated in the § 5 of its statute, which states, that this information system takes data from the Population Register, Estonian Medical Prescription Center, Health Insurance Information System as well as others and this is achieved via data exchange in X-Road.

Although the aforementioned provision of the Public Information Act obliges to regulate the composition of data and the entities submitting data, the provision isn’t sometimes followed in

44 Tervise infosüsteemi põhimäärus. VVm 14.08.2008 nr 131. RT I, 10.05.2014, 31.
practice. Electronic Sea Information System Statute’s § 3(3) states, that the database takes data from other databases and gives data to other databases via X-Road to fulfill legal obligations. However, the composition of data and the persons submitting data aren’t named. Much of the same applies to § 10(4) of the Information System on Supervision of Estonian Consumer Protection Board Statute, which presents a blanket reference to data submitting entities and therefore, doesn’t adhere to the transparency principle.

Legally, the further processing of data is lawful, since it is allowed by the legislation, such as the Public Information Act. The principle of transparency is regulated in a best possible way, but it isn’t always followed in practice. Thus, the principle of lawfulness is complied with, but the principle of transparency could be ensured better, if the statues establishing an information system would always constitute, which composition of data and the entities submitting this data is exercised during the secondary processing of data.

3.2.2. Reuse of data (purpose limitation)

Art 6(4) of the GDPR regulates the secondary processing of data or reusability of personal data for other purposes than stated at first hand. It states, that further processing of data is allowed, when the further processing is based on consent or European Union or Member State law. The further processing is allowed by § 43(2) of the Public Information Act and the reuse of data is being obliged by the § 13 of the General Part of the Economic Activities Act. Additionally, the proactive administrative procedure is encouraged in the Administrative Procedure Act and the Government of Republic Regulation “Principles for Managing Services and Governing Information”.

Technically, it is done by compulsory interoperability and security readiness. The discretion of giving access to data is concluded by the provider of data services. Therefore, the provider of data services is responsible for the compliance of further processing with the purpose limitation principle. The provider has to verify whether the further processing is in accordance with art 6(4) of the GDPR and there exists a legal basis and a purpose for processing the data. If the provider (controller) concludes, the data requested is broader than needed for achieving the...

48 Tarbijakaitseameti järelevalve infosüsteemi põhimäärus. MKMm 07.03.2016 nr 19. RT I, 08.03.2016, 13.
aforementioned purpose, it may deny access to a database. Consequently, the purpose limitation of further processing in Estonia’s data exchange is susceptible on the discretion and competence of the data controller.

3.2.3. Integrity and confidentiality

The integrity and confidentiality is achieved via technical and organizational means. Technically, the § 7 – 11 of the X-Road regulation stipulate the conditions of secure and standardized data exchange between information systems. For example: only verified software for security servers is allowed to be installed, encryption is used on all communication and certification and electronic stamping services are used. X-Road enables to prove, if and when a specific data exchange took place, which is achieved via e-stamps and logs. 49 Organizationally, the provider of data services determines if the user is allowed to exchange data with it. There are lots of different providers, which means, that informational power is distributed between different organizations (providers of data services). Hence, the integrity and confidentiality of data exchange via X-Road is achieved via technical and organizational measures, such as distribution of providing different data, secure connections and the compulsory compliance with technical specifications and RIHA metadata.

3.2.4. Data minimization

Data minimization is one of the key GDPR principles to be followed when implementing OOP. Estonia has observed the data minimization principle by provisions in the Public Information Act. It’s § 43⁶(1) states the definition of “basic data”, which is created in the process of performance of public duties of the administrator of the database. This data is then reused by another database belonging to the State Information System, according to § 43⁶(2). The availability of certain data as basic data is reliant on the documentation entered to the administration system of the state information system or RIHA, as stated in § 43⁶(3). The principle of reusability of basic data is also referenced in the § 5(1)(3) of the Regulation on the Administration System for the State Information System⁵⁰, which states that once collected basic data has to become a source of data for other established databases. Through cataloging the databases and information systems as well as basic data contained in the databases along with the prohibition to establish separate databases for the collection of the same data, as stated

50 Riigi infosüsteemi haldussüsteem. VVm 28.02.2008 nr 58. RT I, 29.03.2016, 6.
in § 43\(^3\) (2) of the Act, positive effect on the implementation of data minimization principle is achieved.

3.2.5. Data accuracy

The objective of RIHA is to ensure the interoperability of public sector information systems and the re-use of technical, organizational and semantic resources, so as to give a clear view of the State registers and the services provided by them.\(^5\) According to § 43\(^6\) (1) and (3) of the Public Information Act, the uniqueness of data and the status of data collected as basic data is determined via technical documentation on the information system entered into RIHA. This means that through RIHA, the non-duplication of same data collection is achieved. Directly, it influences the data to be more accurate, since the data subjects, data collectors and data inserters are more observant, when processing data. Indirectly, the data which is entered only once, cannot be in conflict with data in another database, therefore, creating a possibility to give greater legal meaning to this data. When data is given legal signification, the accuracy has to be higher per se, since there can be forthright consequences stemming from data collected.

3.2.6. Other principles of GDPR

The principles of storage limitation and accountability are not directly applicable to X-Road, since it is a data exchange layer, not a database itself. Storage limitation is set by the data controller on the basis of legal regulations. Therefore, neither X-Road nor RIA has any influence on the execution of this principle. From the viewpoint of accountability, X-Road resembles a torrent-tracker sharing torrent links: not storing any data itself, merely being an intermediary or transport vessel of messages in standardized form between legally significant organizations\(^5\). Since the data controller (service owner) is accountable for data processing and X-Road is a unified separation and data exchange layer\(^5\) between the actual controllers and therefore at most a data processor, it does not have to comply with the principle of accountability.


\(^5\) Kütt, A. Architecture of X-Road. 2014. Available at: https://www.ria.ee/riigiarhitektuur/blog/2014/10/07/architecture-of-x-road/index.html

The X-Road solution adheres to the principles of GDPR due to its technology, architecture and legal framework. Legal instruments postulate the framework for security and protection of personal data. Organizational structure allows the division of power and increased responsibility of data controllers. Technical solutions allow to implement the legal and organizational solutions behind X-Road enabling the reusability of data.

One of the visible problems with the X-Road solution is the transparency of secondary data processing, since at times the composition of data and the entities submitting data isn’t clearly stated in the governing statute of an information system. Consequently, the data subject might not be able to easily discover that a certain institution is processing a certain type of data on him. Legally, the regulation is appropriate, but the implementation has to be supervised more efficiently, so that the data subject’s rights are ensured to full extent.
Conclusion

Public administrations in Europe are bound for a change: implementation of the “once-only” principle will lead to more efficient provision of the public sector services, because data will be shared by different agencies, offices and administrations. The implementation of the principle has to be in accordance with GDPR and this research paper has explored the possible issues of compliance.

From the aspects of the GDPR, the secondary processing of data should be legislated in a clear way, so that data subjects’ rights are ensured. A register of information systems has to be created, which holds the information on which data types are held in which database. The compliance with the purpose limitation principle is reliant on the legal ground for secondary processing: if the ground is stipulated by legal regulations, the principle is observed. The data minimization principle is followed, when a codified list of base data is developed, which specifies the types of data allowed for exchange and further processing. Data accuracy may be achieved via creating a possibility to report false data and an accurate machine-translation of base data in the databases. The aspect of storage limitation has to be concluded from the types of data stored, as certain data has to be ever present, such as data on hereditary diseases. The integrity and confidentiality of data is achieved via technical and organizational means, which include pseudonymization, encryption, electronic stamping and organizationally the data controllers’ discretion of sharing data. The best solution to comply with the accountability principle is for the technical implementation of the OOP to be decentralized and not include any data itself, which would create clarity, as the responsibility for managing databases would only be held by the data controllers and not an intermediary organization, which would be a data processor in the sense of GDPR.

Estonia has been a staple of digitalization and effective electronic governance. The research paper has concluded, that OOP has always been in the core of developing the e-services in Estonia. The legislation concerning OOP has found its way into many laws and regulations, which support the proactive, digital-by-default and privacy-by-default doctrines of Estonian administration. The exchange of data between different databases is built upon X-Road, a data exchange layer of information systems.
X-Road resembles a peer-to-peer system, being the perfect intermediary between various agents of collecting and reusing data. It is decentralized and provides a technically secure and standardized channel for exchanging data between databases and information systems. The secondary processing of data via X-Road was analyzed and following conclusions were made.

The lawfulness and transparency of processing personal data is achieved through the legal regulations, which oblige to specify the different aspects of data processing in the statutes establishing information systems. The purpose limitation principle is achieved via regulating the further processing of data in the statutes and enabling the implementation via technical solutions. Integrity and confidentiality is achieved by standardizing the technological means, restricting access to the data exchange layer and a clear responsibility regulation of the data controller. The storage of data in one location, the specification of base data, cataloging the databases and the presumptive reusability of data assure the compliance with data minimization and accuracy principles of the GDPR. The storage limitation is governed by different laws and neither X-Road or the managing entity have no influence over it. Such is also the case with accountability, since X-Road only facilitates data exchange and has no controlling authority on the data itself.

Having analyzed the compliance of X-Road with GDPR, the author concludes that no major issues are present and the main principles of data protection are adhered to. However, the improvement may be made in the precise regulation of further processing in order to ensure the best compliance with the transparency principle of the GDPR.
References

Literature and studies


   Replacement-PUBLIC.pdf
12. Tupay, P.K. Mikiver, M. E-riik ja põhiõigused. Juridica 2015/3. Available at:
14. WP29 Opinion 15/2011 on the definition of consent, 2011. Available at:

Estonian legislation and statutes

2. Elektroonilise mereinfosüsteemi põhimäärus. MKMm 12.06.2013 nr 39. RT I, 
6. Tarbijakaitseameti järelevalve infosüsteemi põhimäärus. MKMm 07.03.2016 nr 19. RT I, 
    08.03.2016, 13.
7. Teenuste korraldamise ja teabehalduse alused. VVm 25.05.2017 nr 88. – RT I, 
    31.05.2017, 7.

European legislation

   2016 on the protection of natural persons with regard to the processing of personal data 
   and on the free movement of such data, and repealing Directive 95/46/EC
   2014 on electronic identification and trust services for electronic transactions in the 
   internal market and repealing Directive 1999/93/EC
Policy documents


Other documents

1. Algtekst. Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seadus 1027 SE. Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1cb8151b-c5d2-3f1b-8665-489d7ac1c56b/Avaliku%20teabe%20seaduse%20ja%20sele%20seonduvate%20seaduste%20muutmise%20seadus
2. Andmekaitse Inspektiooni peadirektori seisukohad uue andmekaitseöiguse kontseptsiooni asjus, 2017. Available at:


5. Estonian data exchange layer for information systems (X-Road), 2017. Available at: https://scoop4c.eu/cases/estonian-data-exchange-layer-information-systems-x-road


8. Majandustegevuse seadustiku üldosa seletuskiri. SE 806. Available at: https://m.riigikogu.ee/tegevus/eelnoud/eelnou/ea272fce-517d-efd0-0274-b1b8247c5de5/

9. X-Road. Available at: https://cyber.ee/en/e-government/x-road/

10. X-Road. Available at: https://e-estonia.com/solutions/interoperability-services/x-road/

11. X-Road. Factsheet. Available at: https://www.ria.ee/x-tee/fact/#eng