TABLE OF CONTENTS

June 2024

1. Governing Texts

1.1. Legislation

The main piece of data protection legislation is the Personal Data Protection Act 2018 (PDPA), which was adopted on December 12, 2018, and entered into force on November 1, 2023.

The PDPA implements certain national margins of maneuver allowed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), transposes the Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680) (the Law Enforcement Directive), provides the procedure for the exercise of state supervision over compliance with the requirements for processing personal data, and regulates the liability for the violation of these requirements.

The PDPA and the GDPR were implemented by the Act Implementing the Personal Data Protection Act (only available in Estonian here) (the PDPA Implementing Act), which changed data protection provisions in 127 legislative acts in various fields of law to bring them into compliance with the GDPR.

The Estonian data protection authority, the Data Protection Inspectorate (DPI), has issued some general guidance on data transfers (only available in Estonian here).

1.2. Case law

The DPI has not dealt with data transfer cases extensively but has analyzed the lawfulness and transparency of transfers on some occasions.

In the case concerning Living Minerals OÜ (only available in Estonian here), the DPI issued, in March 2021, a precept, according to which the controller had not complied with Article 13(1)(f) of the GDPR, which establishes that the controller has to inform the data subject of the fact that the controller intends to transfer personal data to a third country or international organization and provide the data subject with information about the grounds for the transfer. The DPI ordered the controller to make this information available to data subjects by way of a privacy notice.

In the case concerning AS Kliinik Elite (only available in Estonian here), the DPI issued, in February 2024, a precept according to which the transfer of personal data was in contradiction with data protection principles. AS Kliinik Elite, the controller, is a provider of non-invasive prenatal tests. Although the tests are taken in Estonia, the interpretation of test results takes place outside Estonia, namely in

Croatia and China (Hong Kong). The DPI found that there is no adequacy decision regarding Hong Kong and that there are no other appropriate safeguards provided when transferring personal data to Hong Kong. Nor did the controller obtain data subjects' consent before the transfer.

The DPI has indicated that there have been a number of other cases where the DPI has investigated data transfers. Most of the times, no infringements have been detected, but according to our knowledge, the DPI has also discovered in some other proceedings that the controllers have used US-based service providers without having the appropriate data transfer mechanisms in place. However, these cases have ended without a binding decision of the DPI, as the controllers agreed to stop using the existing service providers and decided to switch to services based in the European Economic Area (EEA).

2. Definitions

The definitions of Article 4 of the GDPR apply for the purposes of the PDPA. This includes the following definitions:

Personal data: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Third party: A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, is authorized to process personal data.

Please note that 'data transfers' are not defined in the GDPR nor in the PDPA, but the concept has been dealt with by the Court of Justice of the European Union (CJEU). The judgment in *Maximillian Schrems v. Data Protection Commissioner* (C-362/14) and the CJEU's Opinion 1/15 on the Envisaged Agreement between Canada and the European Union on the Transfer and Processing of Passenger Name Record Data suggested that an international data transfer occurs when data is sent or made accessible across national borders. The GDPR does not restrict all international data transfers but only transfers to third countries outside the EU and the EEA. Furthermore, the European Data Protection Board (EDPB) issued Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, where it has clarified three cumulative criteria to qualify data processing as a data transfer in the meaning of the GDPR. Namely, a processing is qualified as a data transfer if:

- the controller's or processor's (exporter) processing is subject to the GDPR pursuant to Article 3 of the GDPR;
- the exporter discloses personal data subject to the processing to other controllers or processors (importers) by transmission or makes it available in other way; and
- the importer is in a third country or is an international organization. It is irrelevant if the importer is subject to the GDPR for the given processing.

3. Scope of Application

The territorial scope of the PDPA encompasses the territory of Estonia. The GDPR is directly applicable where the controller or processor is established in the EU or where the processing of personal data of data subjects who are in the EU is carried out by a controller or processor not established in the EU, if the processing activities are related to the offering of goods or services to such data subjects in the EU, or the monitoring of their behavior as far as their behavior takes place within the EU.

As to its material scope, the PDPA applies to the extent that it elaborates and supplements the provisions of the GDPR, and to the extent it regulates the processing of personal data by law enforcement authorities in the prevention, detection, and proceedings of offences and execution of punishments.

The personal scope of the PDPA is analogous to the personal scope of the GDPR, but the PDPA and the GDPR apply to offense proceedings and judicial proceedings with the specifications provided by procedural law, and to constitutional institutions insofar as this concerns the performance of their constitutional duties and is not regulated in the specific acts that concern them.

4. Restrictions on the Transfer of Data

4.1. Within jurisdiction/region

Not applicable.

4.2. Outside of jurisdiction/region

The cross-border data transfer restrictions of Chapter V of the GDPR directly apply to Estonian law. In addition, the PDPA transposes the cross-border data transfer restrictions of the Law Enforcement Directive into Estonian law.

5. Data Localization

There are no generally applicable data localization or residency requirements. However, there are some sector-specific requirements for data localization (see section on sector-specific requirements below).

In addition to sector-specific requirements, the Estonian Information System Authority has issued guidelines that prescribe requirements for the use of cloud services by public bodies who are chief processors (i.e., data controllers) of databases (database is defined as a 'structured body of data processed within an information system of a public body established and used for the performance of functions provided in an act, legislation issued on the basis thereof or an international agreement'). According to the guidelines, if storing of specific public data is permitted within a cloud, then it must always be hosted in the EEA. Furthermore, depending on the risk evaluation and impact analysis there may be a need to store certain data or provide certain services only on the physical servers located in the territory of Estonia. The DPI has also participated in the pan-European monitoring on the use of cloud services by public bodies by the EDPB in 2022. In the final report of the coordinated enforcement action, it was noted that Estonian public bodies are using cloud service providers to process personal data (sometimes special categories of personal data). However, they do not always carry out Data Protection Impact Assessments (DPIA) prior to the use of cloud services. Often, using

the cloud service relies on the trust of the service provider's standard terms. Most organizations have relied on the possibility of selecting data centers in the EU for data processing, meaning that there is allegedly no data transfer to third countries.

Even though there are no mandatory data sovereignty rules, some types of data (e.g., state secrets and classified information) may be kept only on physical servers or media located within the Estonian territory in practice.

6. Sector-Specific Restrictions

Some sector-specific restrictions apply to data transfers in addition to the conditions set out in the GDPR.

Electronic communications

Under the Electronic Communications Act 2005, the providers of telephone or mobile telephone services, the providers of mobile telephone network services, and the providers of internet access, electronic mail, and internet telephony services are required to preserve certain data in the EU. Such data includes, among others:

- the number of the caller and recipient of the call;
- the subscriber's name and address;
- date and time of the beginning and end of the call;
- IMEI of the caller and the recipient;
- the service used;
- the data identifying the geographic location of the cell;
- name and address of the subscriber to whom an IP address, user ID, or phone number is allocated; and
- date and time of the log-in and log-off of the service.

Electronic communications undertakings are also required to store some data only in Estonia. Such data includes:

- information about and replies to data requests of investigative bodies, security authorities, and several other public authorities, including the DPI;
- requests and log files on surveillance agency's or security authority's access to communications networks; and

- data requests by courts.

In addition, the hardware and software used in the provision of communications services in a communications network must not pose a risk to national security. Upon assessing whether the risk is high, it should, *inter alia,* be considered whether personal data are protected in the country of domicile of the producer or provider of maintenance or support services.

Insurance activities

Under Section 85(8) of the Insurance Activities Act 2015, an Estonian branch of a third-country insurance undertaking is required to organize accounting concerning operations in Estonia pursuant to Section 17(2) of the Accounting Act 2002 (i.e., to follow the directly applicable standard in the financial reporting) and to store in Estonia all documents related to operations in Estonia.

Vital services

Under the Emergency Act 2017 (Emergency Act), if information systems ensuring the operation of a vital service are located in a foreign country, the provider of the vital service is required to ensure the continuous operation of the vital service also in a manner and by means not dependent on information systems located in foreign countries. In practice, this may lead to sector-specific data localization requirements. Vital services under the Emergency Act include electricity, natural gas, and liquid fuel supply, the operability of national roads, phone, and mobile phone services, data transmission, digital identification and digital signing, emergency healthcare, payment services, cash circulation, district heating, water supply and sewerage.

The list of providers of vital services will be expanded with the transposition of the NIS2 Directive (Directive (EU) 2022/2555) (the NIS2 Directive). The NIS2 Directive will likely be transposed with the Cybersecurity Act 2018 (Cybersecurity Act). The Directive must be adopted to Estonian law by October 17, 2024, but as for now, the preparation of the new draft law amending the Cybersecurity Act has stalled. Thus, it is highly likely that the transposition of NIS2 Directive will be delayed in Estonia. In summary, under new rules, enterprises will have to notify of any incident that has a significant impact on the provision of their services (significant incidents). They shall also take appropriate and proportionate technical, operational, and organizational measures in order to guarantee the security of network and information systems the enterprise uses. Such measures shall include, for example incident handling, policies on risk analysis and information system security, business continuity and basic cyber hygiene practices and cybersecurity training.

7. Data Transfer Solutions

7.1. Legislative exceptions to the restrictions

The exceptions of Chapter V of the GDPR apply (see, e.g., Article 49 of the GDPR).

7.2. Usage of data transfer agreements/standard contractual clauses

The requirements of Chapter V of the GDPR apply. The DPI has not adopted standard data protection clauses pursuant to Article 46(2)(d) of the GDPR.

Moreover, the European Commission (the Commission) published, on June 4, 2021, its Implementing Decision (EU) 2021/915 of June 4, 2021 on Standard Contractual Clauses between Controllers and Processors under Article 28(7) of Regulation (EU) 2016/679, which lays down new sets of standard contractual clauses (SCCs) for controllers and processors to use for international data transfers. However, as per the CJEU's judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18)* (the Schrems II Case) and the EDPB's Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (the EDPB Guidance), relying only on SCCs might not always be sufficient. Instead, it must be assessed whether the protection afforded to the transferred personal data under the transfer tool (such as SCCs) is equivalent to that guaranteed under the GDPR. If there is anything in the law or practices in the third country that may impinge on the effectiveness of the safeguards provided by the transfer tool (in this case, SCCs), then supplementary measures should be implemented, or the transfer should be suspended. The supplementary measures should be identified on a case-by-case basis,, and they may depend on a number of factors (see section 2.4. of the EDPB Guidance).

7.3. Usage of intragroup agreements, BCRs, CBPRs

The requirements of Article V of the GDPR apply. Binding corporate rules (BCRs), i.e., personal data protection policies for transfers within a group of undertakings or groups of enterprises engaged in a joint economic activity, can be a basis for lawful transfers of personal data provided that the requirements of Article 47 of the GDPR are met. Namely, the BCRs must contain specific information listed in the GDPR, they must be legally binding and enforced by every member of the group, and expressly confer enforceable rights on data subjects.

The EDPB has issued Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR).

7.4. Usage of whitelists and international treaties

General

The requirements of Chapter V of the GDPR apply. The whitelist contains the countries and organizations on which the Commission has adopted an adequacy decision pursuant to Article 45 of the GDPR. The Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, the United Kingdom, Switzerland, Uruguay and the US (commercial organizations participating in the EU-US Data Privacy Framework) as providing an adequate level of personal data protection.

EU-US data transfers

After the CJEU invalidated the EU-US Privacy Shield with its judgment in the Schrems II Case, the Commission and the US announced, on March 15, 2022, that they had confirmed an agreement in principle for a new Transatlantic Data Privacy Framework to facilitate data transfers between the EU and US. On October 7, 2022, the US enacted a presidential Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (Executive Order), directing the steps that the US would take to implement its commitments under the new EU - US Data Privacy Framework (EU-US DPF), and Regulations establishing the Data Protection Review Court (Regulations). In response to the Executive Order and the Regulations, the Commission released, on December 13, 2022, its draft adequacy decision for the EU-US DPF (Draft Adequacy Decision). The Draft Adequacy Decision follows the Commission's assessment of the U.S. legal framework, which includes the Executive Order and the Regulations. The EDPB published its Opinion 5/2023 on the Draft Adequacy Decision. The EDPB noticed a general improvement but at the same time also expressed some concern and a need for clarifications. At the same time, the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE Committee) presented a motion for a resolution in which it opposed the Draft Adequacy Decision.

Subsequently, on July 10, 2023, the Commission voted to adopt its adequacy decision for the EU-US DPF (Adequacy Decision). In particular, the Adequacy Decision concludes that the US provides a level of protection essentially equivalent to that of the EU for personal data transferred under the EU-US DPF from a controller or a processor in the EU to certified organizations in the US. The Adequacy Decision has the effect that personal data transfers from controllers and processors in the EU to certified organizations in the US may take place without the need to obtain any further authorization.

For further information, see Schrems II Portal. However, the Adequacy Decision has received criticism, meaning that it is possible that the Adequacy Decision will be challenged in the future as well.

Exchange of data by security and law enforcement agencies

In addition, Estonia has signed up to the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities (the Declaration) which clarifies how national security and law enforcement agencies can access personal data under existing legal frameworks.

Specifically, the Declaration's principles set out:

- how legal frameworks regulate government access;
- the legal standards that should be applied when access is sought;
- how access is approved and how the resulting data is handled; and
- efforts by countries to provide transparency to the public.

Furthermore, the Declaration also outlines requirements for oversight and redress, providing that there should be mechanisms for effective and impartial oversight to ensure that government access complies with the legal framework, and that the legal framework should provide individuals with effective judicial and non-judicial redress to identify and remedy violations of the national legal framework.

7.5. Other solutions

The requirements of Chapter V of the GDPR apply. According to the GDPR, personal data may also be transferred to a third country or an international organization based on the following safeguards:

- legally binding and enforceable instruments between public authorities or bodies (Article 46(2)(a) of the GDPR);
- approved codes of conduct pursuant to Article 40 of the GDPR, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Article 46(2)(e) of the GDPR);
- approved certification mechanisms pursuant to Article 42 of the GDPR, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (Article 46(2)(f) of the GDPR); and
- subject to the authorization of the DPI, by:
    - contractual clauses between the controller or processor and the controller, processor, or recipient of the personal data in the third country or international organization (Article 46(3)(a) of the GDPR); or

- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights (Article 46(3)(b) of the GDPR).

7.6. Notification/approval requirements for the above

The requirements of the GDPR apply. If the transfer is based on Article 46(3) of the GDPR (*ad hoc* contractual clauses or provisions to be inserted into administrative arrangements), the DPI's authorization is needed. The DPI applies the consistency mechanism referred to in Article 63 of the GDPR and asks for the opinion of the EDPB.

8. Sanctions

Misdemeanor proceedings

Under the Personal Data Protection Act, a violation of the data transfer requirements established in the GDPR is punishable by a fine of up to €20 million or up to 4% of a legal entity's global annual turnover of the previous financial year, whichever amount is higher. The fines are applied by the DPI and can be challenged in general court (not administrative court). Please note that while the GDPR allows the calculation of fines based on the revenue of the entire group of the infringing entity, Estonian law only allows to take into account the revenues of the specific entity. It is possible that both the natural person who directly committed the infringement and the legal person whose interests the natural person acted for are held liable simultaneously.

The fines set out in Article 83 of the GDPR are applied in misdemeanor proceedings in Estonia, as Estonian law does not allow to impose administrative fines. Recital 151 of the GDPR specifically addresses the issue of Danish and Estonian legal systems not allowing for administrative fines.

The recital states that the rules on administrative fines may be applied in such a manner that in Estonia the fine is imposed by the supervisory authority in the framework of misdemeanor procedure, provided that such an application of the rules has an equivalent effect to administrative fines imposed by supervisory authorities.

Before November 2023, it was not possible to apply fines higher than €400,000 for infringements of the GDPR, as pursuant to the general part of the Penal Code (which provides the general rules applicable to misdemeanor and criminal proceedings), the maximum fine for a misdemeanor could be

up to €400,000. However, amendments of the Penal Code entered into force on November 1, 2023, and now, the law stipulates that the maximum threshold
Since the PDPA, as *lex specialis*, foresees higher fines in the amounts provided in the GDPR, the maximum fine set out in the Penal Code does not apply. It must be noted that this applies only to infringements that have taken place since November 1, 2023.

Since November 1, 2023, the statute of limitations for misdemeanor offenses resulting from breaches of the GDPR is three years (as opposed to the previous two years). Moreover, before the amendments of the Penal Code entered into force, fining a legal person always required identifying a natural person who is responsible for the infringement and whose actions can be attributable to the legal person. To ensure compliance of Estonian national law with EU laws, this principle was changed. According to the new wording of the Penal Code, the legal person may be liable for infringement of the GDPR if an infringement has been committed either:

- by any natural person according to instructions given by the legal person's body, its member, a senior official, or a competent representative; or
- due to insufficient work organization or lack of supervision by the legal person.

If a legal person is obliged to act under the law, it will be responsible for its inactions or omissions irrespective of whether or not a natural person was also obliged to act.

In practice, the DPI has so far successfully imposed only marginal fines. There is no publicly available information about fines having been imposed for failing to comply with data transfer rules. The low level of fines can at least partially be attributable to procedural law constraints that had existed in Estonian penal law for quite some time. However, since November 1, 2023, the aforementioned rules apply and it should be possible to impose larger fines in Estonia. The case law in this area is still developing.

Administrative proceedings

If a controller or processor is infringing the data transfer rules, the DPI is authorized to initiate administrative proceedings. The DPI has the competencies listed in Article 57 of the GDPR. In addition to those, the DPI can warn controllers and processors that intended processing operations are likely to infringe on the GDPR and the PDPA. If the DPI finds that the situation could be remedied, it can issue a precept to the controller or processor to demand the rectification or erasure of data or termination or restrictions (both permanent and temporary, including prohibitions) on the processing of personal data. If necessary, for the prevention of damage to the rights and freedoms of natural persons, the DPI can apply organizational, physical, or IT security measures.

If the infringing entity does not comply with the precept, the DPI can apply penalty payments of up to €20 million or up to 4% of the total global annual turnover of the undertaking for the previous financial year, whichever amount is the higher. Please note that unlike in misdemeanor proceedings, for penalty payments, the global turnover is taken into account, not just the turnover of the infringing entity. The penalty payments can be applied repeatedly until the precept is complied with. Both the precepts and the decisions to issue penalty payments can be challenged in administrative court.