GUIDELINES

For implementation of the General Data Protection Regulation

Consolidated version as amended on 08.01.2021.

CONTENTS

KEY CONCEPTS

Key concepts and abbreviations used in the Guidelines are defined here. If a concept is not explained here, it is used as defined in the General Data Protection Regulation:

Processor	A cooperation partner of a credit institution (natural or legal person) which pro cesses personal data held by a credit institution on behalf and in the interest of the credit institution
Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data
Data protection officer	A specialist who qualifies as a data protection officer according to the requirements of the applicable laws
Data subject	▪ A customer of a credit institution (including performers of commercial activities, potential customers, ultimate beneficial owners, related persons, warrantors, cooperation partners that are natural persons, authorised persons or any other identified or identifiable natural persons, whose data are processed by a credit institution) ▪ Employee, candidate whose data are processed by a credit institution
DSI	Data State Inspectorate
Data	Any information relating to an identified or identifiable data subject. Data are defined as any information that provides any data about an identifiable data subject, including objective data such as a person's first name, last name, personal identification number, address, telephone number, bank account number, or bank account information such as payments and turnover; as well as subjective information about the data subject, such as a person's psychological history, person's belonging to a risk group, person's credit rating. Information is considered to be data in any form – i.e. in print, electronic, photographic, audio or video recording data form, as well as set as biometric data
EEA	European Economic Area
EU	European Union
FCMC	Financial and Capital Market Commission
Special Categories of data	Data that reveal a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, or biometric data (if it is used for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation
Credit institution	A member of the Finance Latvia Association
Latvia	Republic of Latvia
AML/CFT Law	Law on the Prevention of Money Laundering and Financing of Terrorism
Controller	A credit institution on whose behalf and in the interest of which data are processed and which is responsible for data processing
GDPR	Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Third party	Any person other than a data processor or the controller or an employee of a controller or a person directly authorised by the controller, who is processing data for their own purposes.
Third country	Any country other than member states of the EU or EEA
Supervisory authority	The Data State Inspectorate or other supervisory authority, in accordance with the GDPR
Guidelines	The current guidelines for ensuring compliance with the General Data Protection Regulation
Article 29 Working Party	The Data Protection Working Party established by the Article 29 of Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data
EDPB	European Data Protection Board – EU body established in accordance with Chapter VII, Section 3 of the GDPR – the successor of the rights and obligations of the Article 29 Working Party

1. INTRODUCTION

These Guidelines have been developed to help credit institutions in understanding the regulatory framework of the GDPR and to assist compliance with its requirements, thus ensuring lawful processing of personal data in day-to-day operations of the credit institution.

The GDPR was adopted on 27 April 2016, and, in accordance with Article 99 of the GDPR, it entered into force on the twentieth day after its publication in the Official Journal of the European Union, that is, on 24 May 2016; Regulation came into effect as of 25 May 2018. There are no derogations as to effective date, therefore since 25 May 2018 it is directly applicable and fully binding to all data processing within or outside the EU, if services or goods are offered to data subjects in the EU or their behaviour is monitored within the EU.

As of May 25, 2018 data protection supervisory authorities have the right to exercise the authority vested in them by the GDPR, including new conditions and requirements of the Regulation, e.g., conducting investigations; requesting information from the controller or processor; issuing warnings; carrying out inspections; applying temporary or permanent bans on data processing; and imposing administrative fines.

1.1. The purpose of the Guidelines

The aim of these Guidelines is to facilitate a shared approach among credit institutions in complying with data protection requirements, as well as to improve cooperation with the supervisory authority and other institutions; consolidate understanding about the responsibilities and rights included in the GDPR; and ultimately to improve the business environment and financial services in Latvia.

These Guidelines facilitate understanding of data protection requirements and their influence on the financial sector. The recommendations are not absolute in their character and are not legally binding; it is a document of a purely informative nature. Implementing the Guidelines will facilitate compliance with the requirements of the GDPR at the level of individual institutions. The requirements of the GDPR provide an opportunity to review and improve current data processing procedures. Revision of data processing procedures, even before the deadline for compliance with the GDPR, may facilitate optimisation of internal processes and management of compliance risks.

A new regulation can sometimes produce confusion about how to understand and apply the new norms. These Guidelines help to develop a shared approach to crucial aspects of data protection in the financial sector, as well as to align the interpretation with the practice of supervisory authorities.

The GDPR provides not only for passive adherence to the requirements, but also for organisations to be able to prove to supervisory authorities their consistent compliance with the provisions of the GDPR – e.g., adhering to the principle of accountability. These Guidelines include recommendations that will help credit institutions adhere to the principle of accountability.

The GDPR prescribes that a data processor and controller is obliged to cooperate with the supervisory authority in various situations. Hence the Guidelines include recommendations on cooperating with the supervisory authority in order to ensure a shared approach. The Guidelines aim to provide consolidated information on an advisable course of action that could facilitate successful mutual cooperation.

The GDPR pays special attention to the principle of transparency. It implies that credit institutions inform the data subject about the data processing activities and render these activities as transparent as possible. To ensure sustainable implementation of this princi-

ple, it is essential to understand what information and by what means should be provided to data subjects, so as to ensure clear and plain communication, thus strengthening customers' and other individuals' trust in the credit institution as data controller. By implementing this principle a credit institution can demonstrate to its customers and a wider public its accountability and commitment to data protection. This could offer a competitive advantage in the financial sector, when compared to actors who do not regard protection of their customers' data as a priority.

Recital 39 GDPR states that the principle of transparency is based upon a requirement that all information and communication relating to personal data processing has to be easily accessible and easy to understand, and that clear and plain language must be used. These Guidelines help credit institutions in developing a shared approach to communication with data subjects on matters relating to data processing and provide an opportunity to clearly demonstrate the work undertaken to comply with the norms of the GDPR.

1.2. Rationale for the Regulation, the legal basis

Until May 25, 2018, data processing in Latvia was carried out according to the Personal Data Protection Law that introduced the requirements of a Directive. The directive was adopted on October 24, 1995. More than 20 years have passed since then. It is a very long time considering the pace of technological development. Advent of digital technologies has considerably reshaped the business environment. At the same time, the pace of technological development brings new challenges in the field of personal data protection.[1]

Currently, technology allows credit institutions, businesses, government institutions and others to use, store and process personal data on an unprecedented scale and at unprecedented speed. Consumers' surveys reveal substantial concern about the safety of their data and their will to exercise more control over the storage and use thereof.

Personal data protection has a pivotal role in the Digital Agenda for Europe and Europe 2020 Strategy. Growing use of digital technology and electronic services implies processing massive amounts of data, based on which decisions are made and personal profiles created. This can lead to both positive and negative consequences for data subjects, highlighting the need for new data protection mechanisms.

A number of EU member states transposed the Directive and used derogations provided for by the Directive. It created diverse practices as national legislation enacted distinct requirements for data processing. General principles were interpreted variously in different countries. It made exercising freedom to provide services thorough the EU more difficult for businesses, thus underlining the necessity for new regulation. To ensure identical legal requirements in all EU states, it was decided that the new legal act would take the form of a Regulation.

Unlike the Directive, the GDPR is directly applicable in all EU member states and it imposes obligations for personal data processing specifically on the data controllers. The GDPR requires the establishment of one or several supervisory authorities in each member state (or for existing institutions to be adapted). These institutions will cooperate within a single network of supervisors to ensure a shared approach to controlling data processing and data security throughout the EU.

The GDPR also introduces certain changes in contrast to the previous legal regulation. For example, data controllers had to register high-risk data processing with a national supervisory authority, but since the GDPR became applicable on May 25, 2018, this is no longer required. Instead, controllers shall keep internal records of data processing and identify high-risk personal data processing activities. If risks cannot be minimised, the data controller shall consult the supervisory authority.

[1] See also the opinion of the European Data Protection Supervisor: https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_en.pdf

The GDPR introduces new measures to ensure the rights of data subjects, such as the right to data portability, the right to object, a requirement to register personal data breaches and to inform the supervisory authority accordingly.

The GDPR does not create a revolution in the field of data protection; it is rather the result of the evolution of data protection environment and technologies. The GDPR retains the key data processing principles and regulatory concepts already enshrined in the Directive, while extending the aims and solutions of the Directive so as to reflect the current levels of risk in digital environments and adapt to the current situation and technological developments.

1.3. The Regulation's place in the legal system

The right to private life is a universally recognised basic human right, enshrined in Article 8 of the European Convention on Human Rights, as well as in Article 7 of the Charter of Fundamental Rights of the European Union (which, according to the Treaty of Lisbon, is legally binding on member states). The right to data protection stems from the right to privacy, but data protection is also fundamental to the successful realisation of other rights, such as freedom of speech. However, the right to the protection of personal data is not an absolute right and it can be restricted to defend important public interests or legitimate interests of other individuals.

The right to data protection is enshrined in the Charter of Fundamental Rights of the European Union as well as in Article 16 of the Treaty on the Functioning of the European Union. The Treaty also recognises the right to the protection of personal data as an independent element of human rights in the EU, not just a part of the right to privacy.

1.4. Applicability of the GDPR

The GDPR is a legal act that is directly applicable in all EU member states, thus ensuring the same legal requirements in all EU member states. Although the GDPR is generally applicable, it allows for member states' derogations. Hence, data protection regulation may still not be fully harmonised across the member states. Credit institutions shall comply with the GDPR directly; however, in cases when the Latvian legislation provides for any additional rights or obligations concerning data processing, a credit institution shall comply also with the national legislation.

During the meeting with the GDPR Working group of the Finance Latvia Association on 21 May 2018, the Data State Inspectorate expressed the opinion that the data of legal entities are beyond the scope of the GDPR. An exception thereto could be the data of self-employed persons, as such data are not included in public registers. However, the context of the cooperation must be assessed on a case-by-case basis, and, if it involves commercial activity, the data of self-employed persons may be treated as legal entity's data. The DSI also recommends considering the attribution of legal entity's representatives (natural persons) data to the respective legal entities and the use thereto for the needs of the given legal entities. For example, the elaboration of a list of wealthy persons would be considered the processing of personal data.

During the meeting with the GDPR Working group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate provided an opinion that the GDPR should not be applicable to ATM (automated teller machine) withdrawals because of absence of the automatic processing element. Nevertheless, the contracts with cooperation partners should contain requirements regarding service provision and confidentiality.

1.5. Scope of the Guidelines

Providing financial services necessarily involves processing personal data of numerous natural persons. Hence, in most cases, credit institutions can be regarded as controllers that process significant amounts of data. Moreover, in connection with provision of financial services personal data can be sent outside the EU and EEA. Hence, and to safeguard the legitimate interests of their customers, credit institutions are obliged to maintain high standards of safety, lawfulness and adequacy, when engaging in processing activities.

Providing financial services involves various partners, such as corresponding banks, international supervisory bodies, payment service providers and providers of a creditworthiness information. Hence cooperation with companies – data processors – to whom credit institutions entrust data processing, as well as the issue of data transfers to third parties, require special attention.

The needs of the credit institutions may vary according to their size – i.e. universal financial service providers – banking groups operating throughout the region will have the needs different from smaller players servicing a narrower circle of customers. It also depends on the specifics of the services and products provided.

To provide services and service the business needs, credit institutions often use IT systems of complex and varied structure. They also require measures of enhanced security along with other measures ensuring data processing in accordance with the current regulation, including the GDPR.

Along with the GDPR, credit institutions have to comply with a large number of other legal acts, adopted both at the national level (laws, regulations of the Cabinet of Ministers, regulations of the Financial and Capital Market Commission), as well as at the EU level.

1.6. Addressees for the Guidelines

These Guidelines were developed to assist members of the Finance Latvia Association in complying with the GDPR. The Association represents banks registered in Latvia, branches of foreign banks, and other financial institutions (associate members) that have united on a voluntary basis to form an association.[2]

For the Finance Latvia Association members these Guidelines will serve as a tool to ensure GDPR compliance in form and substance when providing financial and other services in Latvia. Associate members of the Finance Latvia Association are recommended to implement the Guidelines in as far as they are applicable to their business.

[2] https://www.financelatvia.eu/asociacija/par-asociaciju/

2. PRINCIPLES RELATING TO DATA PROCESSING

This chapter lists and briefly explains the key principles relating to personal data processing that are enshrined in the GDPR. As all GDPR requirements are based on these principles, they are explained in detail in following chapters of the Guidelines.

2.1. Lawfulness, fairness and transparency

A credit institution conforms with these principles in its day-to-day operations to ensure fair treatment of data subjects, processing their data in good faith. The principle of fairness encompasses all other principles, as all of them are aimed at ensuring fair treatment of the data subject by a credit institution, including, but not limited to informing the data subject about data processing and not using their data for purposes other than those they were collected for.

In the regular course of business, fair treatment is manifested as the institution demonstrates respect towards the data subject's interest in protecting their privacy; by supporting and facilitating the exercising of the data subject's rights, for example, by providing the data subject with a simple access to information about the processing of their data, secure storing the data subject's data, allowing for correction of inaccurate data, etc.

When processing data, credit institutions must take into account the data subject's maturity and age, as well as other personal characteristics. Credit institutions must not use the customer's personal deficiencies or incompetence to achieve their purposes.

The principle of fairness is ensured by transparency of data processing. A credit institution ensures that the data subjects are informed in a complete, accurate and convincing manner about the data processing expected and its consequences, if there are no restrictions on the disclosure of such information. Moreover, this information must be provided to the data subject in a concise, plain (with regard to the data subject's maturity and other characteristics, for example, when addressing children or senior citizens), transparent and easily accessible form. In this way, the data subject will be properly informed and aware of the nature and consequences of data processing. This implemented, the processing will have no significant impact on the data subject's privacy.

Lawful data processing means that the credit institution selects purposes for processing the data responsibly, avoiding the emergence and realisation of purposes that could unreasonably impact the data subject's privacy. Purposes are recognised as lawful if they are deemed socially proportionate and are legally permissible.

Lawfulness also implies initiating data processing only on an adequate legal basis. Before any collection or disclosure of customers' data to third parties, as well as before changing the purpose of data processing, a credit institution has to assess the applicability of any of the legal grounds mentioned in the GDPR. If Special Categories of data (such as data concerning a person's health, ethnicity, religious beliefs, or biometric data) or data on a data subject's criminal convictions and offences are being processed, a credit institution must make sure the case meets the special GDPR requirements that allow for processing of such data.

More about implementing this principle – see Section 3.2. of these Guidelines.

2.2. Purpose limitation

To comply with this principle, credit institutions must critically assess the basis of every data processing case, whether future or existing. Data cannot be processed without an

evident and current purpose for such processing. Credit institutions must not carry out data processing without due comprehension as to when and how the collected data will be used, they must not collect data for vague future purposes whose necessity cannot be justified and the initiation of which cannot be supported by law, decisions of the management of the credit institution or internal normative acts (such as procedures and instructions).

This principle also implies the importance of establishing of the initial purpose of data collection, and in cases when the purpose has been changed and is no longer compatible with the initial purpose, the lawfulness of data processing must be re-evaluated.

For more about implementing this principle – see Section 3.1. of these Guidelines.

2.3. Data minimisation

The data minimisation principle – also referred to as the principle of proportionality, adequacy or commensurability – states that the declared lawful purposes shall be reached with the minimum data necessary for the processing.

Complying with this principle means processing only the data necessary to achieve a defined purpose, thus minimising the amount of data processed. In the day-to-day operation of a credit institution this involves reviewing existing administrative tools and processes and limiting access to data to only those departments that need it to fulfil their functions. This will allow for identifying data processing which is redundant for ensuring functions of the institution. Re-evaluation of practices allows to prevent excessive data processing. This provides opportunities for demonstrating a credit institution's compliance with the principles laid out in the GDPR.

Implementation of this principle entails continuous work – data processing cycles shall be regularly assessed for compliance, as the requirements of the legal acts and the business environment and other relevant conditions can change over time.

The data minimisation principle is equally binding for data processing within the credit institutions as well as in cases when data are transferred to other data processors (for example, by minimising the amount of transferable data or pseudonymising it) or disclosed to third parties.

For more about implementing this principle – see Section 4 of these Guidelines.

2.4. Accuracy

Accuracy of data is one of the core values of the GDPR, as only accurate data can allow for adequate and fair decisions to be made about the data subject. Moreover, inaccurate data can cause severe negative and unfair consequences for the data subject. For example, if a credit institution reports inaccurate data about a customer's delay in repaying a loan to the Credit Register of the Bank of Latvia or credit information bureaus, this customer can face restrictions in accessing other credit products not just at the credit institution in question as well as at other credit institutions.

Implementing this principle in good faith is not only a duty of a credit institution, it is a necessary precondition for running its core business. Hence, credit institutions must develop tools to ensure data accuracy both upon its initial collection and when the data are updated to reflect changes in the customer's telephone number, last name, address or identification number. This can be ensured, for example, by including in contracts an obligation to inform the credit institution about changes in data, as well as by comparing data with other databases, inviting customers to review the accuracy of their data via the internet bank etc.).

The GDPR also allows for a proactive participation of a data subject in ensuring the accuracy of their data – by initiating the correction of the data collected by a credit institution or by requesting the collected data from the credit institution, assessing the accuracy and lawfulness of its processing and then requesting for the data to be corrected if they are found to be inaccurate.

The rights of the data subject and the possibilities for exercising those rights as enshrined in the GDPR shall be taken into account when developing internal procedures and tools for ensuring data accuracy in the credit institution.

For more about the implementation of this principle – see Section 5.3. and 6 of these Guidelines.

2.5. Storage limitation

The principle of storage limitation requires that data are stored only for as long as they are necessary for fulfilling the purpose justifying their collection. Once it is fulfilled, the data must be deleted or data carriers – destroyed.

However, this principle needs to be addressed thoroughly. When one purpose has expired, other lawful purposes may arise, and these may justify the retention of data even after the initial purpose has expired. For example, when a service agreement with a customer has expired, its main purpose – providing a service to the customer – has been fulfilled, thus rendering further processing unnecessary. However, the data can be retained to implement other purposes, such as complying with the requirements of the legal acts on retention of accounting documentation, or for protecting the legitimate interests of the credit institution if the former customer decides to dispute transactions or services provided. In cases when the purpose of data processing changes, the scope of data processing necessary to fulfil the new purpose must be reassessed. It is therefore essential to introduce procedures and measures for the re-evaluation of the scale of data processing in case of the change of purpose.

For more about the implementation of this principle – see Section 4.3. of these Guidelines.

2.6. Integrity and confidentiality

Nowadays data processing mostly occurs using digital means. It provides important benefits of efficiency; however, it can also create risks for data subjects. Therefore, a credit institution must pay special attention to the technical and organisational measures of data processing, in order to minimise as much as possible the risks created by technology (such as third parties accessing data or unlawful destruction of data).

The GDPR requires that when processing personal data, the appropriate technical and organisational measures shall be used to ensure data security and protect the data from unauthorised access or alteration, and from unintended destruction or damage.

The GDPR does not provide for specific instructions to credit institutions on how to organise data processing in compliance with the Regulation or ensure the security of data; it is the responsibility of a credit institution to assess potential risks and their impact on data subjects, and to choose appropriate technical and organisational means and measures to minimise or eliminate the risks.

For more about the implementation of this principle – see Section 6 of these Guidelines.

2.7. Accountability

The GDPR assumes that the data subjects do not always possess effective means of controlling their data or substantiating their claims about unsecure or unlawful data processing by the controller (as they often lack the required information or skills). That is why the GDPR shifts the burden of proof of full compliance with its requirements from the data subject to the data controller.

To realize this principle, even before initiating data processing, a credit institution has to develop solutions that clearly demonstrate its compliance with the GDPR, including ensuring data security, providing possibilities for data subjects to exercise their rights, as well as assessing and eliminating the risks.

Compliance can be demonstrated by, for example:

1) introducing technical and organisational measures (i.e., developing internal regulation, carrying out audits of internal data processing procedures, training employees);
2) keeping data processing procedures and instructions up to date;
3) carrying out data protection impact assessments;
4) keeping records of data processing;
5) assigning a data protection officer;
6) implementing the principles of data protection “by design” and data protection “by default”, ensuring minimisation of the processing of personal data and its pseudonymisation, maintaining transparency, enabling the data subject to monitor the data processing, as well as ensuring relevant security measures;
7) implementing relevant codes of conduct or certifying their data processing procedures;
8) ensuring effective cooperation with the supervisory authority.

For more information about the issues covered in this chapter – see Recitals 39, 40, 58, 60, 85 GDPR, and Articles 5, 6, 15 and 25 GDPR.

3. ENSURING LAWFUL DATA PROCESSING

3.1. Identification of purpose

Necessity of having a purpose

Data processing without a pre-defined purpose is not allowed; therefore, prior to commencement of data processing, the purpose of the data processing must be evaluated and specified. A credit institution may have multiple purposes, e.g. employment, provision of services to customer, or ensuring the security of the credit institution. Furthermore, purposes may include sub-purposes necessary to enable the achievement of the main purpose; for example, servicing of customers requires administration of payment for services, compliance with the AML/CFT Law, collection of late payments.

Moreover, the justification of purposes must be re-evaluated at certain intervals, to identify cases where a purpose has been fulfilled and to avoid cases where changes to certain circumstances have obviated the relevant purpose (e.g. regulatory amendments, changes in customer behaviour, changes to the external circumstances that had required the relevant purpose).

Below is a list of likely purposes at a credit institution. However, one should bear in mind that different credit institutions may have different process organisation depending on their structure, the services offered, and other conditions; the following list of purposes is not exhaustive (in particular with regards to Level 2 and Level 3 purposes) and may be expanded or adapted considering the particular needs and circumstances of each credit institution.

Table No. 1

Examples of different level purposes

Level 1 purpose	Level 2 purposes	Level 3 purposes
1. Human resources management purposes	1.1. Personnel selection	
	1.2. Conclusion and performance of an employment contract	
	1.3. Recording working hours	
	1.4. Ensuring the calculation and performance of labour remuneration payments	
	1.5. Adherence to accounting requirements (formatting relevant substantiating documents, recording business trips)	
	1.6. Compliance with legislative requirements (reporting to the State Revenue Service or State Social Insurance Agency, checking whether an employee is a member of a trade union when the employee's employment contract is terminated)	
	1.7. "Benefits package" provision (organisation of health insurance, engagement with business partners to secure discounts for staff)	
	1.8. Recording and monitoring of the fulfilment of operational duties	

Level 1 purpose	Level 2 purposes	Level 3 purposes
2. Provision of the credit institution's services to customers	2.1. Customer identification	
	2.2. Account maintenance/payment service provision:	2.2.1. Payment support
		2.2.2. Issue and maintenance of payment cards/credit cards
	2.3. Provision of credit institution services remotely:	2.3.1. Provision of internet banking services
		2.3.2. Provision of banking services
		2.3.3. Provision of mobile app services
		2.3.4. Use of cookies
	2.4. Provision of lending services:	2.4.1. Assessment of a customer's creditworthiness
		2.4.2. Evaluation of the guarantor's creditworthiness, conclusion of a guarantee contract
		2.4.3. Conclusion of a pledge agreement and assessment of the pledge
		2.4.4. Organisation of contract execution monitoring and loan repayment
	2.5. Compliance with duties specified in the applicable legislation:	2.5.1. Customer due diligence, which includes customer identification, determining the ultimate beneficial owner, determining a politically exposed person
		2.5.2. Reporting to the Credit Register of the Bank of Latvia
		2.5.3. Compliance with requests by state institutions, investigation authorities and other law enforcement authorities
		2.5.4. Compliance with the requirements of the AML/CFT Law, e.g. maintenance of a system for detecting unusual and suspicious transactions
3. Marketing purposes	3.1. Evaluating and researching groups of customers	
	3.2. Sending commercial messages and implementing other communication formats	
	3.3. Organisation of customer loyalty activities	
	3.4. Addressing potential customers	
	3.5. Use of cookies	
4. Risk assessment and prevention in transactions with customers:	4.1. Credit institution risk management	
	4.2. Evaluation of the creditworthiness of customers and other parties	
	4.3. Prevention and detection of fraud	
5. Performance of operational and administrative activities:	5.1. Ensuring security in the premises of credit institutions (e.g. maintenance of access control systems)	
	5.2. Property security (e.g. maintenance of video surveillance systems)	
	5.3. Fulfilment of requirements under the applicable legislation (e.g. adherence to various criteria for credit institution solvency, auditing)	
	5.4. Maintenance of cooperation with business partners, including transfer/receipt of information for the purposes of ensuring cooperation	
	5.5. Debt recovery and collection activities	

Recording of purposes

A purpose must be specified prior to commencing data processing, preferably in addition to confirmation in the form of a decision or decree by the management body of a credit institution, or specification in other internal normative acts of the credit institution (e.g. procedures or instructions), or approval in accordance with other procedures specified by the credit institution, so as to confirm the substantiveness of the new purpose. A purpose must be recorded in the register of data processing activities maintained by the credit institution.

Furthermore, prior to commencing data processing for any new purpose, or making modifications to a purpose, it is advisable to request and obtain an opinion from a data protection officer. If the data protection officer advices against data processing, and further processing takes place contrary to the recommendations of the data protection officer, the credit institution must document the basis for implementing such data processing. In addition, prior to confirming new purposes, it should be evaluated whether such purposes would require data protection impact assessment; however, if a decision is made not to conduct a data protection impact assessment, the rationale should be documented.[3]

Impact of purposes on the data subject

Only a precisely defined purpose can enable a credit institution to ensure adequate data processing in view of a specific purpose (e.g. adherence to the data minimisation principle) and enable lawful data processing – through selecting the appropriate legal basis, and maintaining a good-faith attitude to data subjects and informing them appropriately.

Notification of data subjects about purposes

While evaluating the matter of notifying data subjects about the purposes of processing, the following aspects should be considered:

1. excessively detailed listings of purposes in the information provided to a data subject may prevent the accomplishment of the purpose specified in the GDPR: providing notification to a data subject in a concise, transparent and easily accessible form, using clear and plain language. It is therefore advisable to consider merging some detailed purposes (Level 3 purposes, in the example above) in the notice, for example, by notifying the data subject about Level 1 and Level 2 purposes depending on the nature of the data processing, and providing a more detailed clarification of the purposes upon request of the data subject, or including it in some document available to the data subject (e.g. the credit institution's privacy policy).

2. if the data are collected from third parties (e.g. the receipt of customer due diligence information from public or third-party databases for the purpose of verifying a customer's creditworthiness), and such receipt and/or disclosure of information is intended under EU or Latvian regulations, then, in accordance with Article 14(5) GDPR, the credit institution is not obliged to notify the data subject about such data processing.

Significance (importance) of a purpose

A purpose involving a credit institution must be necessary for the accomplishment of the credit institution's operational objectives; the necessity of implementing the relevant purpose must be immediate rather than based on vague plans for the future. It may be discovered during data processing that the purpose is insufficient, and for this reason re-assessment of the importance of purposes is required with certain regularity, paying attention to implementation of the purposes and the credit institution's attitude with respect to (assessing the importance of) the purposes.

[3] See also Section 6.3 of the Guidelines "Data protection impact assessments".

To keep track of pursuing and achieving purposes, it is advisable to specify the responsible persons or units in charge of monitoring each purpose in the course of processing necessary data, including the periodical reviews of the justification of purposes, and re-evaluation of data being processed to fulfil a purpose.

Change of purposes (further processing)

A credit institution collects data for a specific purpose, and within the framework of this purpose the credit institution must be able to control the data processing being performed, and to ensure data processing in accordance with the originally stated purposes for which the data was collected. If the need arises for a credit institution to use such data for other purposes, the compatibility of a new purpose with the original purpose must be ascertained, ensuring notification of data subjects about the change of purposes if the new purpose is not compatible with the original purposes and the relevant rights of the data subject (e.g. the right to object). If the credit institution wishes to use the data to render a new service to the data subject, it should evaluate whether a new service contract may be concluded with the data subject, thereby fulfilling the requirement to notify the data subject and provide adequate legal basis for the data processing.

Information collected for the purpose of compliance with the AML/CFT Law is to be used in accordance with this purpose; if the purpose is changed (e.g. the information is used to assess creditworthiness), its applicability (e.g. the need to conclude a contract, or legitimate interest) should be evaluated. However, one should keep in mind that it is not always possible to change a purpose – the ability to change a purpose might depend on the sources from which the data are collected. For instance, if the data has been obtained from public sources or from the data subject themselves, after an adequate risk assessment and ascertainment of purpose compatibility has been conducted, the data could be used to evaluate creditworthiness as well; however, if the data for directly ensuring compliance with the AML/CFT Law have been obtained from the State Revenue Service, the data may not be used for any other purpose without specific consent from the data subject and/or from the State Revenue Service.

If the purpose of the intended further processing is compatible with the original purpose of collecting the data, such processing is allowed in the context of the original legal basis. Such compatible purposes may include purposes altered with the data subject's consent, purposes specified in the applicable legislation of the EU and Latvia (e.g. compliance with the law On Accounting, the AML/CFT Law, the Credit Institutions Law, the Consumer Rights Protection Law), and purposes recognised as such by the credit institution based on the evaluation below. Review of purpose compatibility includes the evaluation of at least the following aspects:

1. the link between the original purpose of collecting the data and the purpose of the intended further processing;

2. the context in which the data are collected, paying particular attention to the relationship between the data subject and the credit institution as the controller, e.g. in the case of seniors, who might have a misguided understanding of the nature of the information being requested and the possibilities of using it; loan applicants, for whom their economic situation is at stake; or a labour relationship where the employee has most likely been unable to critically evaluate the necessity of data provision or to object to certain kinds of data processing; or such provision of data was mandatory;

3. the nature of the data, particularly whether Special Categories of data are processed, or data relating to criminal convictions and offences is processed;

4. potential consequences of further processing for the data subject; for example, whether processing the data under the altered purpose may bring about negative consequences (e.g. a negative response to an application);

5. expansion of the amount of data processed;

6. additional guarantees: safeguards that will be provided for ensuring equal rights for data subjects (e.g. data encryption or pseudonymisation, providing the data subject with the right to object to further data processing).

For more information about the issues covered in this chapter – see Recital 50 GDPR, and Article 6 GDPR.

3.2. General legal bases for data processing

The existence of a legal basis (ground) is one of the preconditions for ensuring lawful data processing; it is therefore essential to control the data flow of a credit institution by identifying the legal basis for such flow. As a controller, a credit institution must identify a specific legal basis while processing relevant data. Also noteworthy is the provision of the GDPR specifying that the data subject must be notified about the existence of a relevant legal basis. The following clarifications, grouped by legal basis category, simplify the selection of an appropriate legal basis. In cases where a credit institution processes data as a processor having been assigned the task by a different controller, the credit institution does not require a legal basis for processing the data, to the extent that the data processing takes place within the framework of the assignment given. In this case, the credit institution, as the processor, should maintain a register of such data processing activities.

3.2.1. Consent

"(..) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (..)" [4]

Essence and form of consent

By providing consent, the data subject confirms that data processing can begin, certifying that the data processing is proportionate and consistent with the interests and needs of the data subject. However, the use of consent must be treated with care; for instance, if data must be processed for the purpose of securing a contract performance, consent is not the most suitable legal basis for such data processing, and choosing a different legal basis would be more appropriate. Consent must satisfy the indicators below, which render it suitable for specific data processing activities, e.g. sending of commercial messages, use of internet banking identifiers for third-party services.

Equally, it must be distinguished between consent given in the context of personal data processing and consent which results from Article 62(4) Credit Institutions Law and is attributable to the disclosure of "banking secrecy" for performing a contract entered into with the customer.

The expression of consent is not limited to any specific format and may therefore be obtained:

1. in writing (e.g. by signing a consent document),

2. in electronic format (e.g. by filling out the relevant forms using the internet banking interface of a credit institution),

3. verbally (e.g. by the data subject giving consent during a phone call, subject to the provision of adequate evidence regarding the fact that consent has been given),

4. as an affirmative act (e.g. a customer leaving a business card consents to the processing of the data on the card by the person to whom the business card has been given).

[4] Article 6(1)(a) GDPR.

A credit institution bears the burden of proof that it has obtained unambiguous consent to data processing from the data subject, and maintaining such evidence within the framework of adherence to the principle of accountability.

Valid indicators of consent

For consent to be lawful and valid, it must exhibit a number of mandatory indicators of consent:

1. **"actively given"** – consent must be given by means of an explicit act or clear affirmative action; for example, by actively noting one's choice in a specific field (such as ticking a box), signing a separate consent document, submitting a curriculum vitae (CV) to an employer;

2. **"informed"** and **"unambiguous"** – for consent to qualify as unambiguous, the data subject has to be aware of the purposes for which their data will be processed. For the data subject to adequately assess whether the proposed data processing conforms to their needs, before the data subject expresses consent they must be informed – at the minimum – about the identity of the controller and the processing purposes and where the data processing information may be reviewed in compliance with the GDPR.

   Basic information must be rendered easily accessible to the data subject when asking for consent; thus, a data subject may be deemed inadequately informed if their consent does not include information both about the purposes of data processing and the controller, and their consent form specifies only references to applicable provisions in laws or in the GDPR, or other documents that are not accessible or easily reviewable by the data subject at the time consent is expressed. In this case, at least the aforementioned basic information should be provided at the time the consent is given, although further detailed information could be provided in a separate document (e.g. the general terms and conditions, privacy notice), referred to in the consent document or in another easily accessible location, and the data subject is provided with a simple, accessible way to get acquainted with the relevant document (e.g. it is printed out and issued to the data subject, available on the credit institution's website);

3. **"specific"** – the consent must refer to a specific data processing purpose, about which the data subject has been notified prior to giving consent. If the consent is necessary for several purposes, the credit institution should obtain consent for each purpose separately. However, in case several data processing purposes are bundled and can be pursued only together (e.g. marketing purpose is pursued with profiling) a single consent can be obtained for all data processing purposes. If the consent is included in a document together with other matters, the expression of consent should be distinguishable from the other content, and the data subject should be able to express it independently from, for example, signing a contract;

4. **"free"** – the data subject should have a genuine and free choice, and the data subject may not be forced or misled during the consent process. Hence, it should be evaluated whether the data subject has a freedom of choice in giving a consent – and, if the consent is not received, the data subject will not incur unfavourable consequences, such as a contract with the data subject not being concluded. Likewise, careful consideration should be given to cases where possible inequality may be ascertained in the legal relationship between the data subject and the controller, such as an employee-employer relationship, where the employee might give consent for fear of possible negative consequences, which would render their consent disputable. However, the offering of benefits to the data subject in the form of e.g. discounts, bonuses or additional services – including in cases where an individual consents to the processing of their date of birth so as to receive the opportunity of a discount on partners' services on their birthday – does not in itself mean that consent will be considered to not have been given freely and willingly;

5. **"revocable"** – the data subject has the right to withdraw consent at any time, and it cannot be arranged for the data subject to waive this right. Thus, the correspondence of consent to the essence of the data processing must be evaluated with care. Furthermore, before the data subject gives their consent, they must be informed about the possibility of its withdrawal. During the meeting with the GDPR Working group of the Finance Latvia Association on 7 March 2019 the Data State Inspectorate expressed an opinion that in case information on the withdrawal of consent is already provided, e.g. included in the privacy notice, there is no need to additionally inform the customer on the specifics of giving the consent and its withdrawal options.

   The process of withdrawal must be just as simple as the process of giving the consent; thus, if the consent is received digitally, the same manner must be available for its withdrawal. If the consent is withdrawn, a credit institution cannot further process data for the purposes to which consent is withdrawn, although the credit institution may process the data for other purposes and on other legal bases, e.g. to preserve evidence of consent.;

6. **"provable"** – if the credit institution carries out data processing on the basis of the data subject's consent, clear evidence must be available to the effect that the data subject has consented to the data processing, e.g. by consent recorded on a hard-copy document, recordings of phone calls, or *.log files. Evidence of consent must be stored for the entire period data processing on the basis of the consent, and after the limitation period for potential claims, thereby ensuring protection of the legitimate interests of the credit institution in the event of a dispute on the existence of a legal basis.

Transfer of accountability for consent

Receipt of consent does not relieve the credit institution from the duty to comply with other data protection requirements and principles, including the evaluation of commensurability and ensuring data security – and this must be undertaken prior to receiving consent and commencing data processing.

Likewise, consent cannot legalise any data processing that is prohibited by law or by the GDPR, e.g. processing of data regarding convictions or penalties is only allowed in certain exceptional cases as envisaged in EU or Latvian legislation, or performed under the supervision of an official institution, and the consent of the data subject cannot override this prohibition.

Consent duration

Consent must be received prior to commencing data processing. Consent is valid for an indefinite period, except in cases where the data subject limits the term of validity for their consent in the wording of the consent form. Thus, unless consent specifies a definite term, there is a reason to assume that consent is valid indefinitely, i.e. until the purpose is fulfilled or the consent is withdrawn.

However, recommended practice would be to review the validity of the terms of consent previously provided at certain intervals, given that activities referring to consent may no longer be relevant to the data subject, or the customer may have forgotten about having given the consent; for instance, a customer who is a student may have consented to receipt of news about offers for students made by the credit institution and its business partners. Although the consent has an indefinite term of validity, the customer may no longer find any of the correspondence addressed to students relevant. It is therefore reasonable to periodically review the correspondence of data processing specified in the consent to the needs of the customer, and data processing for such purpose may be suspended or renewed consent may be obtained, or another legal basis may be applied if the purpose of data processing is to be modified.

Consent on behalf of another person

The data subject may only provide consent on their own behalf (with the exception of parent-child relationship and other cases where one's capacity is limited). Expressing consent on the basis of a power of attorney should be evaluated separately, considering the scope of the authorisation.

Table No. 2

Examples of valid and invalid consent:

Valid consent	Invalid consent
In the digital environment, valid consent could include ticking a box (the opt-in principle).	An example of invalid consent in the digital environment would include a tick box that is ticked by default, providing the data subject with the option of unticking it (the opt-out principle).
Sending an internet bank message to a customer specifying that if the customer consents to the use of a new service, they should send confirmation of this consent to the credit institution.	Sending an email or internet bank message to a customer specifying that unless the customer expresses their objections within 10 days, the credit institution will interpret this as a consent to data processing.
The data subject consents to receive information about additional services via email.	The data subject consents to all kinds of processing of their data by the credit institution.
The data subject consents to the use of their phone number for commercial messages, and lack of consent will not negatively affect the service.	Consent is obtained by stating to the customer that the contract will not be concluded unless a consent is given.
Clause 15 on page 3 of the contract states that, by signing the contract, the customer consents to their data being provided to a third party for the purpose of sending commercial messages, and two fields are provided next to the relevant clause of the contract: **"[ ] I agree / [ ] I do not agree"**.	Clause 15 on page 3 of the contract states that, by signing the contract, the customer consents to their data being provided to a third party for the purpose of sending commercial messages, with no further statements included to enable affirmation of consent.

If data processing takes place as a result of the data subject's consent, a credit institution must be able to prove clearly that consent has been obtained in conformance with all of the indicators of the data subject's consent, stated above and mentioned in the GDPR.

The use of consent is recommended in cases where receiving consent is not critical to the maintenance of business processes and/or the provision of services, e.g. for sending commercial messages.

If the consent is revoked, the credit institution has to cease data processing performed on the basis of this consent.[5] In such cases, relevant data are no longer to be processed for purposes for which consent has been withdrawn, although consideration should be given to whether further data processing is necessary for other purposes in view of another legal basis (e.g. retention of data at the credit institution for the purpose of proving to auditors that data processing is lawful or that consent has been given).

For more information about the issues covered in this chapter – see Recitals 32, 42 and 43 GDPR, and Articles 6, 7 and 8 GDPR, and EDPB "Guidelines 05/2020 on consent under Regulation 2016/679" as of 4 May 2020,[6] as well as the Article 29 Data Protection Working Party "Opinion 15/2011 on the definition of consent" as 13 July 2011[7].

[5] See also Section 5.5 of the Guidelines.
[6] EDPB "Guidelines 05/2020 on consent under Regulation 2016/679" as of 4 May 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[7] Article 29 Data Protection Working Party "Opinion 15/2011 on the definition of consent" as 13 July 2011: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

3.2.2. Entering into a contract and performance of a contract

""(...) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (...)"[8]

Necessity

This legal basis gives a possibility to process data prior to concluding a contract, in order to allow for the drafting of the contract, and to carry on processing for as long as the contract with the data subject is in effect. Hence, the recommendation is to process the data necessary for the conclusion of the contract on this specific legal basis, as opposed to consent, for example, which the data subject can withdraw at any time. With regards to data processing based on contract implementation, the data subject is not authorised to prohibit the use of their data to perform the contract while the contract is in effect.

This legal basis would be suitable for sending data to international payment card organisations (MasterCard, VISA etc.) for implementation of a payment (credit) card contract between the customer and the credit institution, and forwarding information to correspondent banks to ensure payments under an account contract concluded between the customer and the credit institution.

The use of this legal basis does not obviate the credit institution's duty to provide the data subject with general information on the processing of their data (see also Section 5.1 of these Guidelines).

Purpose limitation

This legal basis allows for the processing of only that data necessary for contract implementation, e.g. the performance of an account maintenance contract, requiring processing of data on the customer's identity; the account number assigned to the customer; information on account activity and the motivations for it; email address; phone number for contacting the customer in connection with provided services; and other information without which provision of the service would not be possible.

However, if data processing is necessary for other (additional) purposes (e.g. the use of an email address for the sending of commercial messages by third parties, data processing for debt collection activities or customer due diligence), application of this legal basis would not be reasonable, requiring assessment of whether another legal basis may be applied, e.g. consent, the performance of a different contract, the performance of a legal obligation, the legitimate interests of the credit institution or third parties.

Execution of activities prior to contract conclusion

If the data processing is necessary in the course of drafting a contract, it may be performed on the same legal basis without the need to seek another legal basis; however, the amount of data processed should not exceed the amount of data necessary for drafting the contract. Such actions, and the relevant data processing prior to contract conclusion must be directly related to the contract being concluded rather than being based on the legitimate interests of the credit institution.

The following are considered appropriate reasons for processing in the context of this legal basis: collection of information to be specified in a contract or evaluated in the course of drafting a contract; information necessary for identifying the parties to the contract (including information on identification documents and authorisations); data transfer (within the framework of drafting the contract) to other parties to the planned contract, or to their respective representatives.

[8] Article 6(1)(b) GDPR.

The following may be considered inconsistent with this legal ground: data processing necessary for collecting outstanding payments; protection of the interests of the credit institution by referral to court; disclosure of the contents of the contract to law enforcement authorities. In such cases, a more appropriate legal basis might be the legitimate interests of the credit institution or the execution of a legal obligation.

In order to undertake activities prior to conclusion of a contract and to process data on this basis, the data subject must express an intention to enter into the contract or approve drafting the contract. Thus, an inappropriate situation in the context of this legal basis would be the one where the creditworthiness of an existing customer is evaluated in order to offer the customer unsolicited products associated with credit risk. However, in such a case one should consider applying the credit institution's legitimate interests as a legal basis.

If the contract is not concluded following the preparation of the draft, the processing of data on this legal basis is still considered lawful and may be justified by this legal basis. However, as soon as information is received about the data subject's decision not to conclude the contract, the data used to draft the contract should be deleted, with the exception of cases where evidence must be preserved of the legality of the prior processing – for instance, evidence of the fact that customer due diligence has been performed on appropriately and in compliance with the AML/CFT Law, which, in turn, would be justified by the legitimate interests of the controller or the performance of a legal obligation.

Third party data processing

Bearing in mind that this legal basis allows for processing only of the data of a data subject that is party to a contract and has expressed the intention to conclude the contract, this legal basis would not entail the processing of third-party data related to the contract being concluded (e.g. data on relatives specified in an application to review the customer's creditworthiness, data on (potential) guarantors or pledgors specified in the application/contract, or data on the other party to an escrow account) until the counterparties have taken steps to conclude a contract. The processing of data on such third parties must be governed by the legal basis of implementing the legitimate interests of the credit institution or those of a third party (the customer).

For more information about the issues covered in this chapter – see Recital 44 GDPR, and Article 6 GDPR, as well as EDPB "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects" as of 8 October 2019 [9] and the Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014 [10].

[9] EDPB "Guidelines2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects" as of 8 October 2019: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf
[10] Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

3.2.3. Compliance with a legal obligation

"(..) processing is necessary for compliance with a legal obligation to which the controller is subject (..)" [11]

Essence of the term "legal obligation"

By applying this legal ground, the credit institution does not have freedom of choice or has a limited choice regarding the obligations to which it is subject; therefore, data processing consistent with this legal basis includes obligations under the applicable legislation which means that the credit institution is not permitted to decide on whether to conduct data processing: e.g. the information provision clauses specified in Article 63 Credit Institution, Law; the duty to, prior to concluding a consumer lending contract, evaluate information regarding the consumer's income and expenses under Article 8 (4.1.) Consumer Rights Protection Law; the obligation to conduct customer due diligence under the AML/CFT Law.

Sources of legal obligations

A legal obligation may be imposed by any valid EU or Latvian legal act, including laws, regulations of the Cabinet of Ministers, regulations or instructions by state institutions (the FCMC, the Bank of Latvia, law enforcement authorities, the State Data Inspectorate etc.).

The Finance Latvia Association is taking under advisement the opinion of the FCMC on the numerous laws deriving from the old directives which did not actively deal with data protection issues. Therewith, those situations when the applicable legal norm grants a right, which in essence means a legal obligation, have emerged because of the legal technique (opinion provided at the meeting with the GDPR Working group of the Finance Latvia Association on 7 March 2019).

In the opinion of the Article 29 Working Group, the legal obligation does not stem from recommendations and guidelines of supervisory authorities or general policy guidelines and regulations. Thus, in the given case, data processing activities shall be assessed in accordance with Article 6(1)(f) GDPR.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate urged to treat the matter as per the meaning of the legal obligation. In case the data controller has the freedom of action for attaining the purpose and achieving the desired result, such data processing should be justified by a legitimate interest. For example, the legitimate interest can be used to justify data processing that is carried out by each credit institution according to its own methods and measures, even in case the law imposes a general obligation. However, in case the discretion of the credit institution is limited and in essence the required from them data processing is set in a binding document and they rely on the same resources and harmonised methodology, such processing could be justified by a legal obligation.

In the opinion of the DSI, an alternative solution would be to assess the binding nature of state guidelines and recommendations. In case it is detected, the legal acts impose an obligation. The binding nature is absent in case no penalties are prescribed for the failure to comply with the guidelines or recommendations. The Finance Latvia Association emphasizes that state authorities issue guidelines and recommendations to explain specific legal acts or legal norms. Therewith, the decisions are taken on the basis of a legal act or a legal norm of a higher legal force, whereas the explanatory guidelines and recommendations serve as argumentation. To illustrate, consider "Guidelines for Assessing Consumers' Creditworthiness"[12] issued by the Consumer Rights Protection Centre which, in the opinion of the FCMC, incline more towards a legal obligation (opinion provided during the meeting with the GDPR Working group of the Latvia Finance Association on 7 March 2019).

[11] Article 6(1)(c) GDPR.
[12] https://www.ptac.gov.lv/lv/media/131/download

The source of a legal obligation cannot include duties specified in the applicable legislation of countries outside the EU/EEA or imposed by the decisions of such countries' authorities. In such cases, the fulfilment of obligations should be evaluated using the methodology of assessing and balancing the legitimate interests of the credit institution or third party to which data are transferred against the interests of the data subject.

However, considering that financial services are among the most closely regulated industries, the basis of the legal obligation should certainly be considered to be the one most widely applied – for instance, credit institutions must comply with the following legal obligations applicable to a number of fields:

1. tax administration
2. prevention of money laundering and financing of terrorism
3. maintenance of labour relationship
4. adequate support for corporate governance
5. establishment and provision of internal control system of the credit institution
6. adequate servicing of financial instruments
7. lending to consumers and other persons, e.g. to assess customers' solvency and creditworthiness
8. cyber-security
9. account maintenance
10. mprovision of payment services
11. adequate accounting and audit execution and maintenance
12. implementation of credit institution supervision.

As indicated in Section 5.1. below and derives from Article 14(5)(c) GDPR, the data controller is under no obligation to inform the data subject on the processing of his/her data in cases where the processing of such data is expressly laid down by the EU or Latvian law.

For more information about the issues covered in this chapter – see Recitals 10, 14, 19, 41 and 45 GDPR, and Article 6 GDPR, as well as the Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014[13].

3.2.4. Protection of the vital interests of the data subject or third parties

"(...) processing is necessary in order to protect the vital interests of the data subject or of another natural person (...)"[14]

Vital interests

This legal basis is an exception, applicable only to the protection of the essential interests of parties, such as health and safety. In the case of credit institutions, this legal basis would not be broadly useful but may be applied in certain cases of employee data processing (e.g. when information is collected on the health of an employee, in order to be able to provide them with assistance in the event of a deterioration in their health), and in crisis situations (e.g. if someone has health issues in the premises of the credit institutions, requiring discussion of their health condition with medical personnel).

For more information about the issued covered in this chapter – see Recital 46 GDPR; and Article 6 GDPR.

[13] Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[14] Article 6(1)(d) GDPR.

3.2.5. Compliance with public interest or exercising official authority

"(...) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (...)"[15]

Public interest

Public interest should be established in legal acts, so the application of this legal basis is essentially similar to the legal basis for carrying out a legal obligation, with the only difference being that such objectives in the public interest might be less precisely formulated, allowing partial freedom of choice in decision-making, as opposed to applying the legal basis for a legal obligation. In the activity of credit institutions, reporting possible criminal acts (such as attempted fraud) to investigative bodies upon the credit institution's initiative could occur on this legal basis.

While processing data on this legal basis, a credit institution must check whether the relevant public interest is fully established in the applicable legislation or the credit institution has some freedom in selecting the means and scope of data for the fulfilment of relevant purposes. Thus, it should be evaluated whether the data subject can be informed about the intended data processing. However, one should also consider cases where a legal act precludes the data subject from being informed about data processing that is intended or has already taken place.

Official authority vested in the controller

Official authority must be established in the applicable legislation, providing limited freedom of choice as to decision-making on the scope and purposes of data processing. In the financial services sector, only some exceptions apply where persons active in this sector are granted some official authority by the state in the public interest – for example, the state development finance institution ALTUM can apply this legal basis to certain data processing activities.

The data subject's right to object

This basis means that the data subject's right to object to processing must be respected; if such objections are received, the credit institution must, taking into account the reasons stated by the data subject and the data subject's specific situation, re-evaluate the necessity and proportionality of data processing with regards to the relevant data subject; and must make the decision to suspend data processing if the facts presented by the data subject alter the degree of proportionality with respect to the processing of the data subject's data; or else make a decision to proceed with data processing, if the credit institution can prove in a transparent manner that the public interest is more important than the interests of the data subject.

For more information about the issues covered in this chapter – see Recital 45 GDPR, and Article 6 GDPR, as well as the Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014[16].

[15] Article 6(1)(e) GDPR.
[16] Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

3.2.6. Legitimate interests of the controller or a third party

"(...) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (...)"[17]

Obligation of balance

In order to apply this legal basis, a credit institution undertakes a review of balance, or an interest balancing test, with regard to intended data processing – allowing the credit institution to make a considered, documented, justified decision on the appropriate application of this legal basis. The application of this legal basis is expected to expand in the future, and it is advisable for credit institutions to develop a specific procedure for carrying out reviews and monitoring of this balancing of interests.

The balance test includes at least the following activities:

1. evaluating the significance of the legitimate interests of the credit institution or third party to which the data will be transferred;
2. evaluating the impact on the data subject;
3. planning activities to protect the rights of the data subject.

How can interests be balanced?

The opinions[18] drafted by the Article 29 Working Party include mechanisms and guidelines for testing of the balance of interests, as well as the circumstances that should be considered while it is performed. Accordingly, in the course of balance assessment, a number of aspects should be evaluated.

Evaluation of the legitimate interests of the credit institution or third party

Legitimate interests (interests in processing) should be clearly defined and acceptable in accordance with applicable legal acts, and they should be real and current. Legitimate interests may stem from the applicable legal acts or guidelines of supervisory authorities, from the implementation of various basic rights of credit institutions or third parties (e.g. the right to property, the right to the effective protection of rights and a fair trial, freedom of enterprise, freedom of speech and information), as well as major public interests (e.g. the common interest of the public and credit institutions in ensuring that services cannot be received fraudulently, in preventing criminal acts, in ensuring the protection of depositors and the safety of their deposits), and from the individual interests of the credit institution or third party (e.g. to ensure high-quality provision of relevant services and assessment of risks). The interests of a credit institution or third parties have greater support among the public because these interests take precedence. The importance of interests may be indicated by the rights of the controller or third parties to carry out processing of some data, or to achieve certain purposes, as specified in legal acts (e.g. Article 106(4) Credit Institutions Law stipulates the right of credit institutions, subsidiaries of credit institutions, which provide services involving credit risks, loan and savings companies, and insurers, to exchange information on debtors and the process of satisfying their outstanding obligations).

[17] Article 6(1)(f) GDPR.
[18] See Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7(3.1) of Directive 95/46/EC" as of 9 April 2014.

Evaluation of the impact on the data subject

Following identification and understanding of significance of the legitimate interests of credit institutions or third parties, one should evaluate the counterbalancing interests of the other party, i.e. the data subject. While evaluating the interests of data subjects, one is advised to consider the following questions:

1. **Awhat positive or negative consequences will the planned data processing have on the data subject?** The impact on the data subject will be different if the processing brings about positive consequences for the data subject (e.g. if, as a result of customer profiling, the data subject is given the opportunity to receive the service at a substantial discount), compared to situations where processing brings about negative consequences for the data subject. Thus, in the former case, finding a balance between the interests of the parties is easier, while in the latter the interests of the credit institution need to have much greater weight. The evaluation should also consider the fact that data processing may sometimes bring about both positive and negative consequences, in which case all consequences should be assessed interdependently.

   Substantial risk to the rights of a data subject could be presented by data processing that may cause physical, material or non-material damage, particularly if data processing might result in discrimination, identity theft, the forging of documents, financial loss, harm to reputation, compromised confidentiality of data protected by secrecy, prohibited reversal of pseudonymisation, or any other particularly unfavourable economic or social situation where data subjects might lose rights or freedoms, access to controlling their data, where profiling is carried out, or where the processing involves a large amount of data and affects a large number of data subjects. Hence, if processing is found to potentially cause one or more of such risks, the legitimate interests of the credit institution should be carefully considered, in order to verify that they have sufficient importance.

   Likewise, it is important to consider the individual attitudes of data subjects to some data processing situations; for example, one data subject might respond neutrally or positively to being congratulated on their birthday over the phone, while others might experience negative emotions about this;

2. **what emotional impact might the planned data processing have upon the data subject?** Consider a credit institution organising a charity event to support people in need – and where the event would entail publicising photos. Not all the recipients of aid would be pleased about the publicising of their photos because this would reveal information about their financial difficulties. In such cases, visitors could, for example, be photographed against a photo-op wall, which would ensure that only pictures of those guests who had actively affirmed their consent to publishing would actually be published.

3. **evaluation of the likelihood of risk manifestation.** The probability of a risk may be considered to involve two aspects:

   a) if data processing is aimed at preventing and/or mitigating particular risks (e.g. security, prevention of fraud, prevention of theft), it should be critically evaluated how likely a particular risk is to manifest; the lower the likelihood, the lower the significance attributed to the legitimate interest of the credit institution, and vice versa. If the risk itself is substantial – for example, the loss of the entire customer database – then even a low likelihood of manifestation should not minimise the weight of the credit institution's legitimate interest.

b) the importance of the data, and consequently the security of the data, should be evaluated: the higher the interest of third parties in the data at the credit institution's disposal, the higher their desire to acquire the data will be, and the greater the care the credit institution should take to protect the data. If risks to data security cannot be fully prevented or minimised, one should evaluate whether the data processing should be carried out at all.

4. **types of data and significance of potential consequences in cases of unlawful data processing (e.g. data leaks or deletion)**. The more sensitive the data (including both Special Categories of data and data on convictions, as well as the data subject's concerns over data significant to them, such as information about a customer and their transactions, or the availability of funds in their current account) being stored and processed, the more substantial the legitimate interest of the credit institution or third party must be to justify such data processing. Likewise, various actions must be taken to protect the information being collected – the kind of action to be taken depends on the sensitivity of the data.

5. **reasonable expectations on the part of the data subject**. This evaluates the data subject's attitude to the credit institution and the circumstances under which the data have been collected, as well as whether the data subject could have reasonably expected or assumed that processing of their data would take place in the specific manner used. For instance, information collected for the purpose of customer due diligence in accordance with AML/CFT Law requirements must not be used for marketing purposes, e.g. to study the customer's lifestyle and predict the customer's actions, and accordingly to offer them appropriate services.

6. **the status of the data subject**. This evaluates the impact on certain special groups of society whose capabilities to evaluate and respond to the situation are different from others (e.g. children, seniors, people with disabilities), and whether the data subject is in a subordinate relationship (e.g. is an employee) that might discourage them from fully exercising their rights, due to a desire on their part to avoid a possible negative impact on them.

Additional safeguards implemented by a credit institution to prevent undue influence on data subjects

The result of the balancing carried out in accordance with the factors outlined in the previous two bullet points may be affected by the additional actions taken by the credit institution to protect the rights of the data subject. The more extensive the measures taken, the greater the protection that is considered to apply to the data subject's rights – this may be taken into account in the conclusions drawn as a result of the balance test, establishing whether the legitimate interests of the credit institution or third party are sufficiently important that data processing can be permitted to take place. Such additional measures may include the following:

1. **re-evaluation**. Re-evaluation of the legitimate interests of the credit institution should be periodically undertaken, including re-evaluation of their impact on the data subject. The frequency with which re-evaluation takes place depends on the type and purpose of data processing. The more variable the environment, the more frequently re-evaluation should take place. In addition, the re-evaluation of interests should take place upon the request of the data subject, if they exercise the right to object to the processing of their data;

2. **safeguards**. The greater the potential impact on the data subject, the greater the attention that must be paid to safety measures, including the pseudonymisation or encryption of data, where possible;

3. **data minimisation**. The credit institution should evaluate all possible alternatives for the achievement of its legitimate interests, and should choose the manner of data processing that least affects the data subject and their data;

4. **involvement of data subjects or their representatives**. If possible, it is advisable to involve data subjects and/or their representatives (e.g. a trade union) in the balancing process, in order to establish their opinions regarding the aspects involved in the evaluation;

5. **ensuring the right to object**. If possible, it is advisable to provide the data subject with the right to object to data processing – a substantial tool for substantiating the interests of credit institutions in the balancing process.

Result of balancing interests

The purpose of balancing is not to prevent any negative impact on the data subject (although data controllers need to aim at such goal), but rather to prevent a disproportionate impact upon the data subject. Thus, the legitimate interest of the credit institution may be considered justified in cases where it has a proportionate impact upon the data subject.

Documenting the assessment of interest balancing

Considering the principle of accountability, documenting the assessment of interest balancing is recommended. This will assist with re-evaluating the interests because the justifications for the preceding evaluation will be recorded. There is no requirement to internally coordinate a specific format for each evaluation that is performed (e.g. by seeking board approval) but internal procedures should be in place to allow at least some recording of the outcome of the evaluation. This will provide further opportunities to prove that the evaluation of interest balancing has taken place, and to establish the considerations involved in the evaluation. Such an evaluation may occur as part of the procedure for assessing a business project (including the involvement of a data protection officer).

Table No. 3

Example of the interest balancing process

Factors assessed	Planned data processing: Recordings of phone calls (as part of the telephone banking service) to ensure evidence
Step 1 **Overview of suitable legal basis**	1) Application of Article 6(1)(a) GDPR (consent) – not possible, since the individual has no choice regarding whether to consent or not consent to the recording of the call;
	2) Application of Article 6(1)(b) GDPR (performance of a contract) – not appropriate, since provision of evidence is not required for rendering the service as such, although it is essential for the credit institution to be able to prove performance of the contract in the event of a dispute;
	3) Application of Article 6(1)(c) GDPR (legal obligation) – it is not established in any normative act that a credit institution has the duty to record such calls, with the exception of the Financial Instrument Market Law (in which case this legal basis may be used as the reason for doing so, and a balance review will not be necessary);
	4) Application of Article 6(1)(d) GDPR (vital interests) – no necessity to protection of vital interests established to justify such processing;
	5) Application of Article 6(1)(e) GDPR (public interest or performance of a task) – no significant public interests or management tasks established to justify such processing;
	6) Application of Article 6(1)(f) GDPR (legitimate interests of the controller) – inadequate fulfilment of a contract may bring about the risk of losses for the credit institution if the customer files claims against it. It should be taken into account in particular that the service relates to assets of material value owned by the customer, and that this is a particularly sensitive matter for the customer. The burden of proof upon credit institutions is also specified in the legislation applicable for payment services and electronic money processing. Thus, the credit institution needs to secure itself against potential unfounded claims by preserving relevant evidence of appropriate orders being issued and about the person issuing the orders.
Step 2 **Evaluation of the lawfulness and significance of the credit institution's interests**	1) Preserving proof of the fulfilment of contractual obligations is not prohibited by legislation and, is considered necessary under civil procedure regulations; moreover, it is specified in the legislation applicable to payment services and electronic money processing, and is therefore considered a legitimate interest;
	2) the interest is defined with adequate specificity, and there is no doubt regarding its content;
	3) the interest is current and real, because the credit institution has contracts with customers regarding the provision of the relevant service.
Step 3 **Verification of the necessity of data processing (available alternatives)**	It can be established that the existence of orders given verbally over the phone cannot be proven in any other way except by recording a phone call.

Step 4 Evaluation of the data subject's interests	1) The interests of the data subject are affected because the data subject's phone calls to employees of the credit institution are recorded;
	2) the data are not considered Special Category data, and thus does not warrant increased protection; however, it should be noted that data regarding a customer's identity and financial transactions requires additional protection under the Credit Institutions Law;
	3) the data processing does not focus on vulnerable groups in society (e.g. children, employees or seniors), although such persons may be included in the range of data subjects whose data are processed;
	4) the data will be processed on a large scale – due to the high number of customers using this service;
	5) the data are not intended for public disclosure, except to the customers themselves, or to supervisory authorities, law enforcement authorities or courts, if necessary;
	6) the data will not be used in profiling;
	7) reasonable expectations on the part of the data subject: a data subject should be aware that submitting orders for the transfer of funds is a transaction that carries increased risk, and the credit institution is required to prove the receipt of an order;
	8) if data processing was not carried out, uncertainty would be created within the commercial law and civil law environment, since customers would be able to contest executed transactions, potentially affecting the stability of the credit institution and consequently the entire financial sector (assuming widespread contestation of transactions, whereupon the credit institution would have no proof of receiving and executing the appropriate orders);
	9) if calls were not recorded, the risks to the credit institution would be so substantial that the service itself would not be offered; therefore, it is only the carrying out of such processing that enables provision of the service to the data subject, which is a convenient way for the data subject to access their funds;
	10) additionally, there should be taken into consideration the fact that the data subject has freedom of choice regarding whether to use a telephone banking service where their voice is recorded, or to use other means of submitting orders, e.g. internet banking services or in-person submission;
	11) there is a risk of excessive data processing, i.e. one cannot eliminate the possibility of a customer calling the relevant number for references (for which recording is not required), instead of submitting a payment order; or of the customer providing other information (for which recording would not be required) to an employee of the credit institution, in addition to submitting their payment order. However, the credit institution takes into account that any additional restrictions (e.g. not allowing the customer to submit additional information until they switch to another line that does not record incoming calls) would be burdensome both for the customer and the credit institution, and might threaten the existence of such a service.

Step 5 **Additional measures to balance interests**	1) **data minimisation** – considering that the credit institution's phone number can be called by persons with whom a relevant service contract has not been concluded, by potential customers, or by existing customers concerned with other matters, technical and organisational measures must be taken that would allow the data subject to choose the discussion topic, and, if the topic is fully or partly not subject to recording, to allow the data subject to proceed with the call without recording or identification taking place;
	2) **functional separation** – if calls are also recorded for other purposes (e.g. quality assistance), technical and organisational measures should be implemented to separate call records by purpose, and to prevent the different purposes from being mixed;
	3) **access to pseudonymisation** – evaluate whether the taking of orders can be organised based on customer/user numbers without other data (first name, surname, personal identification number) being recorded during the call, thereby ensuring that, if persons without a legal basis for accessing the relevant data do gain access to the recordings of the calls, the relevant data would remain anonymous, preventing harm being done to the interests of the data subject;
	4) **notification of the data subject** – the data subject must be informed about such data processing in the contract and prior to each recording, in order to ensure the data subject is aware that the data are being recorded, and to enable them to act accordingly;
	5) consider whether an evaluation of the impact on data protection is necessary;
	6) **retention period** – customers may contest transactions for up to 3 years (period of limitation for commercial transactions) or in some cases up to 10 years (general period of limitation); in accordance with the law On Accounting, substantiating documents must be stored for 5 years..
Step 6 **Demonstrating compliance and transparency**	1) provide the data subject with access to information regarding the reasons that indicate that the interests of the credit institution outweighs the limitation of the data subject's rights, including the relevant references to it in the service contract, the general terms, the website and/or in some other manner accessible to the data subject;
	2) preserve this evaluation in document form and provide to the supervisory authority if necessary;
	3) regularly review this data processing procedure assessment, considering the nature and degree of risk inherent to the processing, determining the appropriate periodicity of review at the time of the initial assessment.
Step 7 **Actions if the data subject objects**	1) In such cases, there is no reason to provide data subjects with the right to unconditionally withdraw consent, taking into account that the interests of the credit institution prevail;
	2) If the data subject objects to such data processing (e.g. to storage), the process owner evaluates the arguments provided by the data subject, and whether they alter the outcome of the balancing; if so, the process owner takes appropriate action to modify the processing.
Step 8 **Final decision**	Recognise that the legitimate interests of the credit institution outweigh the impact upon the data subject, enabling the data processing in accordance with Article 6(1)(f) GDPR (legitimate interests of the controller).

The data subject's right to object

When this legal basis is applied, the right of the data subject to object to processing should be honoured. If such objections are received, the credit institution should, upon evaluating the reasons provided by the data subject, re-evaluate the necessity and proportionality of data processing with regards to the relevant data subject, and make a decision to suspend data processing if the facts presented by the data subject change the balance of interests of the two parties with regard to processing the data of the data subject, or to continue data processing, if the credit institution is able to clearly illustrate that its legitimate interests or the legitimate interests of the relevant third party outweigh those of the data subject.

In what cases, if an evaluation of the individual interests has already been carried out, would this legal basis apply?

Use of this legal basis should be considered in the following cases, with a separate evaluation of the balance of interests being carried out:

1. if the processing concerns performance of the contract, although there is a risk that the data processing may not be essential to ensuring the performance of the contract at a basic level;

2. if the data processing is required by applicable legislation of third countries (outside the EU/EEA) or court rulings of third countries with which no mutual legal assistance treaty has been concluded;

3. if the data processing is justified by the guidelines and recommendations of state institutions (for more information – see Section 3.2.3 above);

4. if a legal act stipulates the credit institution's right (discretion) to perform some kind of data processing (for more information – see Section 3.2.3 above);

5. if data processing is necessary for litigation;

6. if the credit institution involves external consultants (e.g. attorneys-at-law, auditors), unless the involvement of such consultants is a specific legal obligation;

7. fraud prevention;

8. protection of property;

9. proof of executed obligations (e.g. phone call records for service quality control);

10. sending data to other company within the same group (in the EU/EEA) for internal administrative purposes, including the processing of customer or employee data;

11. if necessary, to review an employee's conflict of interest situation, particularly where such a review is not stipulated in the applicable legislation.

Another example of data processing that is performed based on the data controller's legitimate interest involves customer surveys that are conducted with the purpose of establishing the customer's opinion on the received services and for taking such information into consideration in order to:

1) improve service quality for the specific customer, and/or
2) improve service in general.

During the meeting with the GDPR Working group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that the purpose and the contents of customer surveys should be taken into account. In case the survey is conducted with the purpose of establishing the customer's opinion on the received service and taking it into account to improve the service quality for a particular customer or for customers in general, such data processing can be justified with the legitimate interest of the service provider. However, in case the survey is carried out for simultaneous promotion of the service provider's image and services, the consent of the data subject should be obtained for such data processing. Similar assessment should be given to greetings sent to customers, e.g. on birthdays. If the service provider is also promoting its image and services when sending the greetings, the data processing should be based on the customer's consent. The DSI considers that there could be a legitimate interest of the service provider to conduct customer surveys or to greet customers on holidays. The DSI did not identify the potential harm to customers through processing of customer data for the purpose of sending greetings or surveys. In the opinion of the DSI, the fact of no risk or minor risk of harming the customer is a significant aspect that must be considered when conducting the balancing test.

For more information about the issues covered in this chapter – see Recitals 37, 41, 48, and 49 GDPR, Article 6 GDPR, as well as the Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014[19].

3.3. Processing of Special Categories of data

Importance of Special Category data

Special Category of data must be processed in accordance with higher security requirements – unlawful processing of Special Category of data may cause substantial harm to the interests of the data subject. Thus, a credit institution should separate Special Category of data from other data and limit access to it, and should set enhanced security requirements for working with such data.

Special Category of data may be encountered in various documents and units of information (e.g. video recordings and photographs), although one should critically evaluate whether such information is intended for use as Special Category of data. Absent of such a purpose, processing of the relevant information should not be considered processing of Special Category of data. For instance, if a video surveillance recording shows a person wearing clothes that could indicate adherence to a religious movement, but there is no reason for analysing this video recording with the specific purpose of using this information, processing of this data should not be considered processing of Special Category of data.

Processing restrictions

In accordance with Article 9(1), the processing of special categories of personal data is prohibited unless any of the exceptions set out in Article 9(2) GDPR apply or the relevant EU Member State has introduced further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

[19] Article 29 Working Party "Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" as of 9 April 2014: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

At the meeting with the GDPR Working group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that in cases when the data subject provides to the data controller special category personal data on his/her own initiative, it can be assumed that the data have been obtained based on the data subject's explicit consent. In case information on the withdrawal of the consent is already included in the data controller's privacy notice, it is not necessary to additionally notify the customer on the specifics of giving consent and its withdrawal options. Moreover, the DSI considers that the risk of violating the customer's privacy is minor in case the data provided by the customer are applied for taking a decision favourable to the customer.

Processing of employee health data and information about an employee's membership of a trade union

Processing of such data is possible on the basis of Article 9(2.b,h) GDPR, which allows for the processing of Special Category of data if it is necessary to fulfil obligations and exercise rights in matters of labour, or to evaluate an employee's capacity for work, as far as this is authorised by member states' legal acts. Thus, one should consider the limitations on processing of such data (data minimisation), mentioned in special legal norms – for instance, under Article 101(6) Labour Law, an employer has the responsibility to establish whether an employee is a member of a trade union only prior to terminating an employment contract; with regards to health-related data, Article 33(4) Labour Law sets out that the employer has the right to receive information on the health condition of the employee only to the extent that this has major significance to the conclusion of the employment contract and the fulfilment of planned work. If an employee is, for example, sent to a health check-up in accordance with Article 36(2) Labour Law, the doctor specifies only whether the candidate is suitable for the relevant work.

Processing of politically exposed persons' data

Processing of such data should be justified by Article 9(2)(g) GDPR, which allows for the processing of data regarding political affiliations in cases where it is of substantial public interest and specified in the legislation of a member state. In this case, reference should be made to Article 25 AML/CFT Law, which sets out the obligation to determine whether a customer or an ultimate beneficial owner has the status of being a politically exposed person.

Biometric data processing

As the processing of biometric data is becoming increasingly common in personal identification and premises access control systems, it should be noted that biometric data fall within the scope of Special Category of data. Thus, such data cannot be processed based on the legitimate interests of a credit institution alone. Biometric data may be used for identification upon receipt of freely given and explicit consent from the data subject, or if the processing of personal data is necessary due to substantial public interest, i.e. if the applicable legislation of the Republic of Latvia specifies this interest and therefore entails the processing of biometric data.

Taking copies of passports

In some cases (e.g. in old passports or foreigners' passports), data that contain Special Category of data (such as data on the ethnicity of the data subject) may also be included in passports. Credit institutions may have to process passport or other identification document data to identify their customers. In accordance with Article 14(1) AML/CFT Law concerning customer identification, a credit institution is obliged to make copies of personal identification documents, including a passport copy, on the basis of which customer identification is carried out. Fulfilment of this legal obligation is a sufficient basis for processing all information contained in the copy of a personal identification document (including an individual's height, and, in some cases, ethnicity – if these are specified).

It should be noted that, in accordance with the principle of data minimisation, in order to accomplish the purpose specified in the AML/CFT Law, a copy of the passport (of the pages displaying basic personal data, and, in some cases, also of the pages displaying residence permit data) is sufficient, and copying other pages of the passport that might contain further information would be excessive. It should also be taken into account that, in accordance with the Regulation of the Cabinet of Ministers No. 134 of 21 February 2012, "Regulations on Personal Identification Documents", a person's ethnicity is specified on the third page of a passport (i.e. on subsequent openings beyond basic data); thus, while making a copy of a personal identification document, a credit institution will not have to process Special Category of data at all.

However, it should be taken into account that there are exceptions with personal identification documents issued abroad and older identification documents issued in Latvia, where Special Category of data may be contained in the opening pages, in these cases such processing will be adequate and legitimate.

Regarding copies of personal identification documents in the context of a legal labour relationship, it should be noted that such a practice may be considered excessive because the legislator has specified in Article 35(1)(1) Labour Law that presentation of a personal identification document is sufficient to identify a natural person. However, the information necessary for proof of identification of an individual may be noted in, for example, a personal index card.

A credit institution as an insurance intermediary

If a credit institution is engaged in insurance intermediation in accordance with the Insurance and Reinsurance Intermediary Operations Law, and within the framework of such intermediation has to process Special Category of data, the credit institution would, in the context of such a relationship, most likely be considered a processor acting in the interest of an insurance company (controller). Thus, the credit institution should conform to the instructions of the insurance company regarding the data being processed, separating the data processed by the insurance intermediary from other data processed by the credit institution, and should maintain a register of a data processor's activities.

For more information about the issues covered in this chapter – see Recitals 35, 51, 52, 53 and 54 GDPR, and Article 9 GDPR.

3.4. Processing of data relating to criminal convictions and offences

Processing restrictions

Processing of data about criminal convictions and offences, or security measures related to them, may be performed only under the control of an official authority, or in the event that the processing is authorised by EU legislation or by member states' national legislation. Thus, data on criminal convictions and offences (including criminal convictions and penalties for administrative violations) may be processed by a credit institution only in cases specified, and to the extent specified, by law.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that in case the data subject provides the data controller with data relating to his/her criminal convictions and offences on his/her own initiative, it may be assumed that the data have been obtained based on the data subject's consent. In case information on the withdrawal of the consent is already included in the data controller's privacy notice, it is not necessary to additionally notify the

customer on the specifics of giving consent and its withdrawal options. Moreover, the DSI considers that the risk of violating the customer' s privacy is minor in case the data provided by the customer are applied for taking a decision favourable to the customer.

Data on criminal convictions and offences in the context of a labour relationship

In order to fulfil the obligation to review a person's criminal convictions, a credit institution makes a request (to the relevant person or to appropriate registers) if the person is to be appointed in charge of compliance with the AML/CFT Law, since Article 10(4) AML/CFT Law specifies that such duties may be fulfilled by a person not convicted of intentionally committing crimes. Furthermore, in accordance with Article 25(1) Credit Institutions Law, a credit institution is obliged to review the conviction data of its board members, as well as of the head of the internal audit service, risk officer, compliance officer, company auditor, head of a foreign branch in Latvia or abroad, and proctor – to verify whether the relevant person has been convicted (or a criminal case has been terminated) in connection with intentionally committing a crime, including bankruptcy fraud. A prohibition on convictions may also be specified in other regulatory enactments and may apply to other categories of employees, such as audit committee members.

Moreover, in accordance with Article 34[5] Credit Institutions Law, a credit institution shall process the data relating to criminal convictions of candidates and employees, considering that a credit institution may not employ persons for the positions that are directly involved in the provision of financial services or credit exposure management or affect the risk profile of the credit institution in case the person has been convicted of committing an intentional criminal offence against the State, property or governance procedures, or of committing an intentional criminal offence in national economy or while in service in a governmental authority, or of committing a terrorism related criminal offence, and the criminal record thereon has not been extinguished or set aside.

Data on criminal convictions and offences in the course of carrying out customer due diligence

In accordance with Article 41(2)(4) AML/CFT Law, credit institutions have the right (and in some cases the obligation) to process the data on the criminal convictions of a customer, a potential customer, ultimate beneficial owners of a customer or representatives of a customer, in the course of evaluating the risk of money laundering and financing of terrorism that the customer carries, as well as in cases where there is a necessity to notify the Control Service about a suspicious transaction, or to refrain from the execution of a suspicious transaction.

For more information about the issues covered in this chapter – see Recital 75 GDPR and Article 10 GDPR.

3.5. Processing of the personal data of children

Specific protection of children

Children (persons under the age of 18, or having reached the age of majority, whichever is later) merit specific protection because they do not have the same legal capacity as a mature person, and may not be fully aware of the relevant risks, consequences or safeguards, or of their rights with relation to data processing. Such specific protections should apply to the processing of children's data performed both by automated means and manually, in a structured manner that does not involve automated means. It is inadvisable to apply automated decision-making to children.[20] If, however, automated decision-making is applied, one must first evaluate carefully whether such data processing might cause harm to the interests of the child. Automated decision-making related to processing of children's data would be acceptable in order to, for example, protect the funds of a child against various risks that the child might be unable to fully prevent or adequately mitigate on their own.

[20] Recital 71 GDPR.

Information provided to children

In communicating with a child, information must be provided to them and communication must take place in language that is sufficiently clear and plain for the child to understand easily. It is also essential to provide information about the rights of a data subject not only to the child's legal representative, but to the child themselves, as long as they are able to exercise some rights in line with the credit institution's practice, independently and without the legal representative's involvement. At the same time, if a child's data are used in a context where the child does not have independent decision-making rights, the controller must ensure that the child's legal representative is notified about the planned data processing.

Use of children's data for information society services

If processing of children's data is intended in the context of information society services[21], based on consent provided by a child, one should consider the provisions of Article 33 Personal Data Processing Law, which specify that a child is entitled to give consent independently from the age of 13, and that the child needs to be informed about the type of data processing for which consent is being given. If the option of using information society services is provided to children under the age of 13, a credit institution must verify that consent has been given, or at least confirmed, on behalf of the child, by a person who has guardianship or custody rights with respect to the child. It is recommended that the procedure for a credit institution to verify a child's consent should be included in the relevant procedure.

As to the degree of certainty that consent has been given or approved on behalf of the child by a person who has guardianship or custody rights with regards to the child, the credit institution must make a reasonable effort to verify this connection. This may be done taking into account the available technologies; an acceptable solution would be one where a previously identified person (e.g. parent) declares in writing their connection to children under their guardianship or in their custody, and authorises their children to perform certain actions pertaining to information society services.

Children's rights to decide with regards to their data in other matters

In general, it should be noted that a child does not have the same degree of legal capacity (beyond the aforementioned exception of giving consent), and therefore the exercise of children's rights should take place with the mediation of parents or guardians, including requests for copies of data, the limitation of processing activities, data deletion, and the exercise of other rights. However, if a credit institution offers specific services to children, it is advisable (taking into account a child's degree of awareness and ability to decide about the exercise of their rights) to evaluate the option of allowing a child to exercise certain rights independently, in so far as this would not present harm to the child. Such exercise of certain rights by children should not restrict the abilities of a child's parents or guardians to supervise the processing of data related to the child and, if necessary, to exercise all of the data subject's rights with regard to the child.

It should further be noted that the GDPR sets out that the aforementioned provisions for the use of children's data for information society services do not affect general contractual rights, including the provisions regarding the validity, conclusion and consequences of a contract entered into by a child. Thus, a child has the right to make decisions regarding their data, e.g. labour relationships (under Article 37 Labour Law, a child may conclude an employment contract from the age of 15) or disposal of a child's individual property in accordance with the provisions of the Civil Law.

For more information about the issues covered in this chapter – in Recitals 38 and 58 GDPR; and Article 8 GDPR.

[21] According to the Article 1(2) of the Law On Information Society Services, information society service is a distance service (parties do not meet simultaneously) which is usually a paid service provided using electronic means (electronic information processing and storage equipment, including digit compression equipment) and upon the individual request of a recipient of the service. Information society services include the electronic trade of goods and services, the sending of commercial communications, the possibilities offered for searching for information, access to this and the obtaining of information, services that ensure the transmission of information in an electronic communication network or access to an electronic communication network, and storage of information.
According to Article 1(1)(b) the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down the procedure for the provision of information in the field of technical regulations and of rules on Information Society services, an Information Society service is any service normally provided for remuneration, at a distance (the service is provided without the parties being simultaneously present), by electronic means (the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means) and at the individual request of a recipient of services.

4. DATA MINIMISATION

4.1. Mechanisms for data minimisation

Essence of the principle

Data minimisation is performed to determine the minimum amount of data and the minimum scope of processing necessary to fulfil the purposes previously specified. In order to verify that data are being processed to the appropriate extent:

1. the credit institution must precisely define the purpose, since only accurately defined purposes enable an understanding of the minimum amount of data and processing necessary to fulfil it. For instance, the purpose of "customer service" is too generally defined: it does not provide an accurate understanding of the minimum necessary categories of data to be processed. If the purpose were subdivided into more specific purposes – "customer identification" (in person or digitally), "maintenance of customer relationships", "provision of a specific service" or "proof of order execution" – then the evaluation of the minimum necessary amount of data to be processed to fulfil these purposes in each specific case would be much more efficient;

2. the credit institution should evaluate all alternatives for fulfilling a specific purpose with minimal data processing, and should select the alternative which involves the least amount of invasion of privacy. For example, if a credit institution wishes to fulfil the purpose of sending customers text message (SMS) reminders about contract performance, collecting customers' email addresses would not be necessary; testing information systems must take place using dummy data, instead of an actual customer database, as using the latter would threaten the accuracy, security, and confidentiality of the data;

3. a decision should be made on the technical solutions for processing, selecting whichever one that least infringes upon the interests of the data subject. For instance, if video surveillance cameras are installed for security purposes, making audio recordings would be a disproportionate measure to determine individuals' access to property, because it would not represent the minimum necessary means of fulfilling the purpose. Furthermore, one should also consider the persons who must access the relevant information to execute their duties – in order that their access and processing rights can be assigned and monitored; the credit institution should ensure, as far as possible, that a person can only access the amount of data that are necessary for fulfilling the duties assigned to them.

Pseudonymisation

Pseudonymisation is a method for processing data in such a way that the data cannot be linked to a specific data subject without the use of additional information, provided that such additional information is kept separate and protected: this may include the use of customer numbers if information about a customer (first name, surname or personal identification number) is stored separately.

This is one of the mechanisms for minimising data processing because persons who access the data would be unable to link the data to a specific individual, and the data may be considered anonymous in this regard. However, in choosing pseudonymisation methods, one should take due care to verify that all identifiers which could allow an individual to be recognised are removed – for example, covering up a candidate's first name, surname and personal identification number on a CV is not sufficient for the data included in the CV to be considered pseudonymised because other information contained in the document (for example, work experience, educational institutions) could be used to identify the individual.

On account of the operational specifics of each credit institution, pseudonymisation might be used in order to, for example, separate pseudonymised data from data that would reverse the pseudonymisation, thereby ensuring that access to the original data does not allow for identification of the individual to whom the relevant information refers. One should evaluate whether the processing of pseudonymised data is insufficient in the context of certain units' duties (e.g. while drafting various internal activity reports of the credit institution); the same evaluation should also be performed with regards to data processing entrusted to the processor.

4.2. Data minimisation for specific purposes

Data storage for back-up purposes

The inclusion of data in back-up copies is sufficiently motivated by the credit institution's legitimate interest in processing the data stored in such back-up copies even if other data processing purposes have been fulfilled. Some data cannot be deleted from a back-up copy, because this could substantially affect the rights of other persons to data preservation: if a back-up copy is compromised, it might fail to serve its purpose – restoring data when necessary – and this would affect data integrity and security. However, a credit institution should specify the frequency with which back-up copies are made, and the number of back-up copies necessary for storage, as well as providing for the deletion of older copies. This would ensure that data are deleted after the fulfilment of the credit institution's lawful purpose.

Documents containing data that have to be deleted at different times

If a document contains data that have to be deleted at different times, or related documents that contain some documents that are to be stored for different periods of time – such as a package of documents signed with a digital signature, consisting of distinct documents with distinct retention periods, or a document that various employees have signed to confirm their acquaintance with a procedure – it is reasonable to store the entire document or document package until the retention period for all such data within the document (or all documents within the package) elapses.

Actions with an employee's digital signature following termination of legal labour relations

If an employee terminates labour relations with a credit institution, thereafter the credit institution should not use features that allow automatic forwarding to a colleague's email address, instead evaluating the possibility of setting the former employee's work email address to reply with automatic notifications to email senders, informing them that the employee is no longer legally engaged in a labour relationship with the credit institution, specifying that the email inbox is not being checked, and inviting the sender to resend their message to an employee who has replaced the former employee.

In this case, whether to disclose the data contained in an email message would be up to the sender of the original message, allowing them to choose, knowing the intent and content of their message, whether to forward the email, or whether not to, as might be decided if the message contains personal correspondence.

Evaluation of a customer's creditworthiness based on information knowingly published by the customer

If the credit institution has a legitimate purpose for collecting data, e.g. in order to evaluate a customer's creditworthiness based on an application submitted by the customer for a service that carries credit risk, such information may also be collected from publicly available sources, including sources where the customer has knowingly published information about themselves (including publicly available social media content). However, as well as taking into account the scope of the processing and its impact on data subjects, the credit institution should consider whether a data protection impact assessment is to be performed with regard to such cases of processing.

Receipt of documents containing extended data

A situation may arise where a credit institution collects information (e.g. from public registries), or a customer provides to the credit institution some documents for due diligence purposes which also contain the data of other data subjects, e.g. cooperation contracts, documents on founding a commercial entity, which also include data on other founders, or various session minutes containing other persons' data. In this case, preserving such a document would be considered proportionate and necessary, because if the content of the document were to be edited (e.g. by deleting the relevant data of other data subjects), it could unduly influence the legal force of the document; therefore, the document may be stored even if it contains other persons' data, as far as this is required for fulfilment the purpose of customer due diligence.

However, if a customer is found to have submitted a document containing other persons' data that are not required for the credit institution to fulfil the relevant purposes (e.g. customer due diligence), the document should be deleted or the data it contains should be covered up, providing that this does not affect the legal force of the document. However, if such third-party data within the credit institution's systems cannot be selected based on the parameters defined by the third party, the relevant processing of third-party personal data is not subject to the requirements of the GDPR or the rights of a data subject.[22]

Monitoring of employees' emails

Regular monitoring of the content of the electronic messages sent by employees is not acceptable (except in cases where such monitoring is justified by, for example, suspicion that the employee is using a corporate email address contrary to internal regulations, if the internal regulations provide for such monitoring; or for the purpose of investigating disciplinary violations). In order to mitigate the impact of monitoring on employee privacy, the use of technical solutions for identifying risks is recommended (e.g. the detection of certain keywords or phrases in the text of an email; or information available to the credit institution regarding threats to the interests of the credit institution, such as disclosure of trade secrets, including data; the existence of a conflict of interest; intended or actual criminal activity; or other substantial threats to the interests of the credit institution). Thus, staff would not be subjected to excessive email monitoring, and data processing would only apply to persons who are suspected to have committed violations during the course of the labour relationship. However, when considering the scale of the processing, the credit institution should evaluate the necessity of carrying out a data protection impact assessment.

[22] Article 2(1) GDPR.

4.3. Data retention period

The duration for which data are retained directly relates to the necessity of using the data for certain purposes. Hence, the factors listed in the table below should be taken into account while evaluating the period for data retention.

Table No. 4

Considerations to take into account when determining a data retention period

Factors	Retention periods
1. Is the data necessary for performing current service contracts?	Data should be retained for as long as the relevant service contract is in effect; some types of data should be stored for as long as business relations with a customer are ongoing. However, in the case of terminating a service contract, one should check whether new justified purposes for retaining the data have arisen (see the factors listed in the Table below);
2. 2. Do the data need to be retained for the performance of legal obligations under the applicable legislation?	In compliance with the statutory retention periods specified in the applicable legislation of the Republic of Latvia, such as: 1) Compliance with the AML/CFT Law – throughout the effective term of the business relations, and for 5 years (or more, if instructed by the Control Service) in the cases specified in Article 37 AML/CFT Law for customer identification documents, information on customers or their accounts, declaration of ultimate beneficial owners, correspondence with the customer and other customer due diligence documents; 2) Compliance with the law On Accounting, i.e. 10 years for registries and documents of accounting organisations, and 5 years for related substantiating documents; 3) In cases specified in the Financial Instrument Market Law – 10 years with regards to the storage of documents substantiating transactions in financial instruments, and other related documents[23]; 4) In cases specified in the Consumer Rights Protection Law – 1 year following the fulfilment of a consumer's obligations under a loan contract to provide documentation related to issuing the loan[24]; 5) Compliance with FCMC regulations and instructions.
3. Do the data need to be retained to protect the interests of the credit institution in the event of various claims following the termination of business relations?	Examples of limitation periods for some claims: 1) **60 years** – limitation period for claims referring to deposits with a credit institution, under Article 71 Credit Institutions Law; 2) **10 years** – general limitation period for obligation rights (Article 1895 Civil Law); 3) **3 years** – claims stemming from a commercial transaction (Article 406 Commercial Law).
STORAGE OF A CUSTOMER'S FILE	Considering that a customer's file (customer's documents that are being stored altogether or separately) may consist of documents with different storage periods, it should be regarded that the credit institution is entitled to store the entire package of documents, including contracts, for the term of 10 years after termination of all transactions with the customer (by respecting the general contract law limitation period set out in Article 1895 Civil Law to protect own legitimate interests in case of any claims).
STORAGE OF A KYC FILE	Article 37(2) AML/CFT Law stipulates that the subject of the law shall store all information obtained in the course of the customer due diligence for five years after termination of a business relationship. After the end of the mentioned period, the aforementioned documents (information) shall be disposed/deleted, unless the subject of the law has received instructions according to Article 37(3) AML/CFT Law to extend the storage period.

[23] Article 124(1.9 and 1.10) Financial Instrument Market Law.
[24] Article 8(5.3) Consumer Rights Protection Law.

4. Do other important legitimate interests exist that would be infringed upon in the event of deletion? (This may include storing data in back-up copies or a data subject's exercise of the right to restriction of processing of their data.)	With regards to the creation of back-up copies, the retention period may be specified as the term for which a back-up copy is necessary. A procedure should be specified regarding how frequently back-up copies are made and what number of back-up copies stored. At the time of deletion of older copies, deletion of data subjects' data should be carried out to an adequate level.
5. Proof of lawful data processing during the preceding period. For example, proof of consent for processing activities performed previously.	Because the applicable legislation does not provide for a shorter limitation period regarding data subjects' claims on a credit institution referring to ensuring lawful data processing, the general civil law limitation period of 10 years applies. Thus, in order to prove that data processing has been organised lawfully, proof of lawful data processing must be stored for 10 years after the data processing is stopped. Equally, in case the consent is provided during a phone conversation, the period for storing the record of the call depends on the set period for storing evidence for granting/receipt of consent.
6. Evidence for lawful data processing in case no contract is signed, but measures have been taken for signing thereof.	Prior to entering into a contract with the potential customer, the credit institution may need to verify the information on the specific person in public registers. With regard to the fact that the data subject has the right to receive information on data recipients' categories for the term of 2 years, credit institutions may have the legal basis (legitimate interest) to store information on information acquisition grounds to prove the legitimacy of such processing. However, such data processing (storage) must be assessed from the aspect of proportionality.

If, while evaluating the specific retention period for data, justifiably different retention periods are identified – e.g. legal acts specify one period for data retention but the credit institution establishes that it requires a longer retention period to protect its interests, there is a reason to retain the data for as long as necessary in order to fulfil all reasonable retention purposes.

While evaluating data retention periods, it is advisable to take into account the Guidelines of the Finance Latvia Association to determine the periods of storage for different documents.

It is advisable to review the need to retain documents/data on a regular basis and look for solutions to shorten the retention periods.

Should the data retained for everyday needs be kept separate from the data retained following the termination of business relations?

It is advisable to isolate the data necessary for everyday needs from those stored for other purposes, and to specify distinct access solutions – thereby reducing the number of people that can access the data and minimising the risk of unauthorised access to the regular-use database.

Repeated evaluation of data minimisation during specification of retention periods

While providing a customer with a service on the basis of, for example, a contract, there is a reasonable need for a certain amount of data to be processed to adequately provide the service; however, while evaluating the retention period following the termination of business relations, one should also re-evaluate the amount of data necessary to be processed to fulfil such purposes, e.g. when preserving data on a customer's transactions in order to protect the interests of the credit institution in the event of various potential claims against the credit institution, it is most likely that it will not be necessary to preserve the credit institution's everyday correspondence with the customer.

For more information about the issues covered in this chapter – see Recitals 28 and 29 GDPR, and Article 5 GDPR.

5. RIGHTS OF DATA SUBJECTS

The controller should provide the data subject with the right to exercise the rights specified in Articles 12–22 GDPR, including the right to information, the right of access, the right to rectification, the right to be forgotten, the right to restrict processing, the right to data portability, the right to object, as well as rights related to automated processing, including profiling, as well as specified in Articles 14 and 34 GDPR, communication related to processing, notifications about data rectification or erasure, restriction of processing, and data protection breaches.

In the opinion of the GDPR Working Group of the Finance Latvia Association, data protection rights should be treated as rights of a personal nature and the implementation thereof requires special authorization. During the meeting with the GDPR Working Group of the Finance Latvia Association on 7March 2019, the Data State Inspectorate provided an opinion that the data subject may authorize another person to perform the request of the data subject. However, to reassure on the true will of the data subject, such authorization must be precise and set out in proper details, i.e. directly attributable to the implementation of the rights granted by the GDPR.

All communication and activities carried out by the controller in accordance with the GDPR or in connection with the data subject's requests should be performed free of charge.

If the controller concludes that a request is manifestly unfounded or excessive, the controller is obliged to bear the burden of demonstrating that. The credit institution performs its assessment based on the specific situation and the specifics of the request made by the data subject. In order to evaluate whether the data subject's request is manifestly unfounded or excessive, the controller may consider and evaluate the following factors:

1. the identity of the applicant and the data subject specified in the request whose data are being requested;
2. the amount of data being requested/rectified, and the resources that would need to be used to process such a request;
3. the content of the request of the data subject, comparing it to historical requests in order to evaluate whether such a request has been submitted and processed previously;
4. the date on which the data subject last submitted a request or contacted the credit institution in connection with data processing;
5. the history of actions taken with the data subject's data, and the regularity of the controller's processing activities/modifications to the data subject's data;
6. the date on which the data subject's data was last rectified, erased or blocked, or on which other actions/changes took place in accordance with a request;
7. whether the data subject has previously received a response from the credit institution to the submitted request;
8. whether the legal justification included in the request, or the set of actual circumstances, has substantially changed in relation to the previous response to the relevant request;
9. other information specific to the relevant request made by the data subject that might indicate that the request made by the data subject is manifestly unfounded or excessive.

Following an assessment of the data subject's request, conclusions should be drawn and the following actions should be taken:

1. if the data subject's request is founded, the credit institution is obliged to react to the request, and to ensure implementation of the data subject's request free of charge

2. if the data subject's request is manifestly unfounded or excessive, the credit institution may:

   a) charge a reasonable fee, specified in the pricelist of the credit institution, taking into account the administrative costs of providing the information or communication, or of taking the action requested (e.g. labour resource costs, information carrier costs or postage service costs – however, no expenses of developing solutions to exercise the rights of data subjects may be transferred to the data subjects themselves, i.e. the specified expenses must apply directly to the specific request);

   b) refuse to act on the request.

In case the request of the data subject is not submitted in the official language or in the language of service of the credit institution, the credit institution may charge a reasonable fee to cover the translation costs or refuse to act on the request.

In order to implement the principle of accountability, one should establish a procedure for processing the requests of data subjects and document the execution of data subjects' requests (including audit trails), particularly in cases where the execution of a request is declined in full or in part, payment for execution of the request is requested, or data are transferred to third parties as a result of the request being executed.

The following subchapters set out the rights of the data subject to which the aforementioned steps for evaluating a data subject's request refer, and provide a credit institution with a way to evaluate the justification for a data subject's request and to define subsequent actions related to handling the request.

5.1. Right to information

General requirements for providing information

In accordance with Article 12 GDPR, the controller provides information on data processing to a data subject:

1. in a concise, transparent, plain and easily accessible form (in writing, electronically, or, upon the data subject's request, orally)

2. using clear and plain language, particularly in the case of information provided to children

3. free of charge, except where the data subject's request is manifestly unfounded or excessive.

Table No. 5

What information should be provided to the data subject?

Information provided:	If the data was collected from the data subject	If the data was not collected from the data subject	Implementation of the right of access (see below Section 5.2 of these Guidelines)
Identity and contact information of the credit institution, and, if necessary, of the representative of the credit institution who is acting as the controller	✓	✓	
Contact information of the data protection officer (if a data protection officer has been assigned), e.g. dpo@institution.lv	✓	✓	
Purposes of processing for which the data are intended, and the legal basis for such processing	✓	✓	✓
Categories of data processed		✓	✓
Legitimate interests of the credit institution or a third party, if the processing is dependent on this legal basis	✓	✓	
Recipients or categories of recipients of the data*	✓	✓	✓
Where applicable – information on data transfer to a third country, and appropriate safeguards to ensure data protection	✓	✓	✓
Data retention period and criteria for determining the data retention period	✓	✓	✓
Information regarding the rights of the data subject (right of access, right to rectification, right to erasure, right to restriction of processing, right to object, right to data portability)	✓	✓	✓
Information regarding the right to withdraw consent, if the processing is based on consent	✓	✓	
Information regarding the right to submit a complaint to the supervisory authority	✓	✓	✓
Information regarding the sources of the data		✓	✓
Information regarding whether the provision of data is a statutory or contractual requirement, and whether there is a prerequisite for entering into a contract, as well as whether the data subject is obliged to provide the data and what the possible consequences of their failure to provide such data would be	✓		
Information on the use of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing	✓	✓	✓

When information is to be provided::	During the receipt of data	1) within a reasonable period following the receipt of the personal data (at the latest within one month); 2) if the data are to be used for communication with the data subject – at the latest at the time of the first communication with the data subject; 3) if the data are intended for disclosure to another recipient – at the latest when the first such disclosure happens.	Without undue delay, and in any event within one month following the receipt of the request (if necessary, having taken into account the complexity and number of the requests, the aforementioned period may be extended by up to 2 months)

* During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 May 2018, the Data State Inspectorate expressed its opinion that the data controller must independently and on a case-by-case basis evaluate what information and to what extent should be provided to the data subject, in case the latter requests information on the data processor in accordance with Article 15(1)(c) GDPR. The DSI considers that it is in compliance with the GDPR to specify only the categories of data recipients without separately indicating each data recipient (name or other identifiers) that could violate the commercial interests of the data controller or processor.

Organising the provision of information

Because the amount of information to be provided is substantial, taking into account the form of communication, one should carefully evaluate which information is to be provided to the data subject either directly or indirectly, because in some cases the provision of all information at once may have the opposite effect, by preventing the data subject from absorbing the relevant information. For instance, regarding notifications about video surveillance, it is not possible for all of the information to be placed on informative stickers or signs, thus according to Article 36(3) Personal Data Processing Law at least the name of the data controller, its contact details, the purpose of data processing and also a reference to the possibility to obtain other information falling under Article 13 GDPR should be given (e.g. reference to the credit institution's website or privacy notice).

It is also recommended that modern methods for delivering information be implemented, such as QR (Quick Response) codes, which allow the data subject to access additional information in a convenient way. Even if the internet is used for communication, the amount of information being provided must be assessed: the information may need to be divided into the part that will be placed in the user area (although the extent of information that can be provided in the active zone on the internet will be much greater than on the video surveillance stickers on the premises) and the part that can be made available in hyperlinks, ensuring that the process required to view such additional information is not complicated, and accessing it is just as convenient as using the active section of a website.

The same model should be considered in the context of communication with a customer in person or in writing, because a data subject will not always be able to assess such information immediately and in an effective way. It is therefore advisable to consider the option of providing essential information either orally or by including it in a written document, while the other part is included in specially created reference materials that can be issued to a customer or appended to, for example, contract documentation. For example, the general terms and conditions could be among the documents which contain information for the customer on the personal data processing carried out by the credit institution.

Likewise, when communicating with a customer by phone, prior to recording the phone call, it is recommended to inform the data subject on the data processing, by giving a reference to the credit institution's website or privacy notice.

Cases where information can be withheld

Provision of information to the data subject is an important element of accountability, and a credit institution should try to inform data subjects about the processing of their data; however, the GDPR also envisages certain exceptions where information about data processing can be withheld from the data subject. Cases where information cannot be provided should be recorded. In accordance with the GDPR, information can be withheld in the following cases:

1. **if the data subject already has the information:** for example, if an additional service contract is being concluded with the data subject, and all information was provided in order to conclude the initial contract. However, one should evaluate critically whether the customer has access to all the necessary information, and whether the controller is able to prove that the data subject already has this information. If it is established and provable that the customer has one part of the information, only the other (missing) units of information should be provided;

2. **if provision of such information is impossible or would require a disproportionate effort**; for example, it would be excessive to provide information to potential pledgors and guarantors based on a received loan application, although once a contract with such a pledgor or guarantor is concluded, relevant information should be provided.

   It is also acceptable for individuals whose data are included in contracts submitted by customers (or collected from third parties, e.g. public registries), and whose data are not primarily intended for processing, not to be notified. The prohibition on notifying a data subject could be justified under the applicable legislation, e.g. within the framework of implementing the AML/CFT Law, a customer must not be notified about reports to the Control Service written with regards to their transactions, and in other cases where the applicable legislation prohibits the notification of a person that data has been provided to prosecutors or courts;

3. **if receipt or disclosure of information is clearly stipulated under the EU or Latvian law:** for example, collection of the ultimate beneficial owner's data stipulated in Article 18 AML/CFT Law, disclosure cases stipulated in Article 63 Credit Institutions Law and the right to provide and receive information stipulated in the Credit Information Bureau Law etc.;

4. **if the data must remain confidential subject to an obligation of professional secrecy regulated by the EU or Latvian law.** This exception primarily applies to state government institutions.

Do the requirements to provide information also apply to customers if the processing of their data began prior to the date when the GDPR came into force?

Execution of the requirements to provide information applies to all data subjects regardless of whether data processing commenced before or after the GDPR came into force. A reasonable solution for informing existing customers/data subjects would be providing information on changes to the scope of the information, and sending the updated information as an email message to customers; placing a notification on the credit institution's platforms for internet banking and other services; and publishing it on the credit institution's website, so that the information is made available to other groups of data subjects – for example, to ultimate beneficial owners or to third parties whose data are being processed to provide services to customers.

For more information about the issues covered in this chapter – see Recitals 58, 60, 61, 62 and 73 GDPR; and Articles 12, 13 and 14 GDPR, as well as EDPB "Guidelines 3/2019 on processing of personal data through video devices" as of 29 January 2020[25].

5.2. Right of access by the data subject

Essence of the right of access by the data subject

This right entitles the data subject to the following:

1. **receiving confirmation of the processing of their data**, i.e. receiving a response from the credit institution to the data subject's request as to whether the data subject's data are or are not being processed. The credit institution is obliged to provide a response even if the credit institution does not process the applicant's data;

2. **accessing the data** – receiving a copy of the data (rather than documents), for example, attaching a print-out from the storage system containing the data subject's data to the response letter sent to the data subject, or stating the scope of processed date in the response letter sent to the data subject;

3. **receiving information about the processing of their data** (similarly to how the right to be informed is exercised).

Purpose of the right of access by the data subject

The aim of this right is to allow data subjects to access their data to verify the accuracy of the data and the lawfulness of the data processing at each stage of the data processing operation. In case the data subject wants to exercise the right to access his/her data and to receive a data copy to be transferred further to another recipient, e.g. court, such a request should not be considered a data subject request within the meaning of Article 15 GDPR.

Data copy

The right of access by the data subject should be exercised with regard to data from data processing systems, not documents; therefore, a data subject may not insist on documents or copies of documents being issued,[26] unless the data subject can justify the specific need to receive a copy of a document, such as where only the content and format of the document can be used to determine the importance of the data and the potential consequences that data processing may have for the data subject. Thus, document copies, duplicates, excerpts and printouts should be issued against a set fee, as the right of the data subject to access his/her data and to receive a copy thereof free of charge that are laid down in Article 12(5) GDPR are not attributable to such cases. Commercial banks may foresee exceptions for specific cases or regarding specific categories of data subjects (e.g. the senior segment).

[25] EDPB "Guidelines 3/2019 on processing of personal data through video devices" as of 29 January 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

[26] See also: Finance Latvia Association, FSA and DPA Infopage "The General Data Protection Regulation: what does it mean to me as a bank client?", September, 2018: https://www.financelatvia.eu/wp-content/uploads/2018/09/The-General-Data-Protection-Regulation_-what-does-it-mean-to-me-as-a-bank-client.pdf

Likewise, the data subject is not entitled to request access to certain files that contain data, even though provision of such access may be one way to guarantee the rights of the data subject.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 May 2018, the Data State Inspectorate expressed the opinion that for the purpose of ensuring the right of access to the data subject within the scope of Article 15 GDPR, the data controller may not limit only to providing a data copy. Namely, the data controller should answer all questions laid down in Article 15 (1) GDPR.

Respect for the rights and freedoms of other persons

The data subject's right to receive data should be evaluated in the context of the rights and freedoms of other parties (including the credit institution and other data subjects): for instance, the data subject would not be entitled to request an unedited video surveillance recording in which the data subject is visible alongside other individuals. Such a recording could only be provided in edited form. As a result of the fulfilment of a request, information containing data of third parties can be provided if the consent of such persons has been received, or if such information is already available to the applicant. In other cases, it should be evaluated whether the relevant circumstances render it acceptable to provide the applicant with the data of the relevant third parties.

One should also carefully evaluate the provision of information to a data subject whose data are contained in documents that justify the operations of another customer (e.g. if within the framework of the AML/CFT Law, a customer submits a contract on cooperation with another individual). The credit institution should be aware that, in issuing unedited information or an unedited document, the credit institution may unintentionally disclose information about the fact that the business partner of the data subjects stated in the contract is a customer of the credit institution, and thereby infringe upon customer secrecy as established under the Credit Institutions Law. Consequently, as the controller, the credit institution should take particular care in evaluating the extent of information disclosure, taking into account that certain data are considered non-disclosable under the Credit Institutions Law.

For instance, the issue of audit trails related to persons that have accessed the data of a given data subject could initially be addressed by simply providing a reference to the categories of data recipients who may access the data (e.g. credit institution staff or processor staff) and by issuing information on a specific individual that has accessed the data subject's data following a request from competent institution (e.g. suspicion of a data leak), thereby protecting, for example, the right of an employee to the protection of their data, including protection of information about them, e.g. about their employment status with the relevant employer.

Periods for the execution of requests

The credit institution provides the requested information without undue delay – in any event, within one month following receipt of the request, it notifies the data subject about the activities performed. Having taken into account the complexity and number of the requests, the period of time available for execution of the request may be extended by up to 2 months. The data subject should be informed about such extension within one month of receipt of their request.

Format for provision of information

Information may be provided to the data subject in various available formats, adjusted to the needs of the data subject. However, one should specify either hard copy or electronic format (such as the internet bank) as the primary format in which information is provided; the option of verbally informing the data subject upon request should also be available. A notable factor in specifying the format is ensuring evidence of fulfilment of the credit institution's obligation. As a matter of good practice, Recital 63 GDPR recognises the provision of a remote access to a system, such as an internet bank, that allows a data subject to get direct access to his/her data.

Taking into account that the data provided must be intelligible, so that the data subject can fully exercise their right to monitor the quality of their data and the lawfulness of processing, in some cases additional information may be appended to the issued data to facilitate their understanding of the importance of the issued data. For instance, if entries or comments relevant to a person have been written in the form of internal code, the data subject should be provided with clarification of the relevant comments.

As people's understanding of data protection improves, the number of data subjects' requests might increase, and credit institutions may have to process a large amount of requests. Furthermore, if credit institutions store some types of data in obsolete systems, automating the systems to guarantee data subjects' right to access their data may prove to be a complicated task. Credit institutions might also hold enormous amounts of data on a customer, and, in such cases, providing the entirety of such data might fail to satisfy the request of a data subject who is a "typical customer", i.e. receipt of information regarding the processing of their data, in an intelligible format.

In view of the aforementioned considerations, credit institutions may shape data subjects' access rights implementation systems with multi-stage approach.

If a data subject's request does not specify the type of data or the scope of the data in which the data subject is interested, the credit institution ensures access to actual main data and provides the data subject with a general overview of the data that are being processed by the credit institution, indicating the data subject's core information – data on their identity, contact details, information on the products used by the customer, as a clear report or noting a way for the data subject to access the information themselves (e.g. via internet bank).

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that in case the personal data can no longer be selected in the system but have been archived, the data subject may be informed on this fact and a fee can be applied for accessing such data.

If the data subject's request indicates a need to access specific information that would not be covered by the initial response, or if after the first-stage response the data subject exercises their right to access some specific information, the request to the credit institution should be processed individually, taking into account the data subject's request, by counting the term for drafting the answer anew. During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that the data controller may inquire about the purpose of the data subject's request and the intended use of such data. When responding to the data subject's request, it should be considered from the data subject's perspective as the data subject is exercising the right granted under Article 15 GDPR in order to rectify, erase or transmit his/her data. Therefore, the credit institution may ask the data subject to specify the extent of information and forms of data processing that are covered by the request and to provide justification for their request (e.g. in cases where, after the initial response,

the data subject requests access to the entirety of their data). The implementation of this right is not affected by whether the data subject has been previously informed about aspects of the processing of their data.[27]

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed the opinion that the personal data contained in the credit institution's memos on the customer or notes to the customer's profile might be compared to the subjective notes of the so-called "Examination Case".[28] Because of the security requirements of the credit institution, the data controller my concurrently also have a legitimate interest to retain the confidentiality of its internal procedures – in such a case the personal data should be separated.

Moreover, the Data State Inspectorate considers that IT sub-systems which support and register who has accessed the data, in particular IT security sub-systems, perform the function of technical solutions and therewith the data contained in these systems are not attributable to the data subject's request within the meaning of the GDPR but instead – are applicable to the data control and the control exercised by the data controller over the data.

Relation to data portability

If the data subject has stated the need to access their data to preserve or reuse it, such a request should be treated as an example of the data subject exercising their right to data portability, and, with regards to the data subject's right to data portability, the requirements for data portability should be observed.[29] If necessary, the credit institution should request the data subject's clarifications regarding the essence and purpose of their request.

Identification of data subjects

An important aspect of exercising this right is adequate identification of the data subject because providing extensive information to the wrong individual may lead to serious negative consequences for the data subject. Attention must therefore be paid to determining the identity of the applicant and to the manner in which the information will be delivered to the data subject (in person, electronically or by post), ensuring identification of the recipient of the data, as well as the security of the data.

Adequate identification would also include digital identification by means of internet bank authorisation issued by a credit institution or sending a registered letter via "Latvijas Pasts" VAS or courier post, or via sworn bailiff or notary – doing this will ensure that the content is issued to the right individual. If data are to be sent via email, in addition to carrying out identification, it should also be verified that the data are being sent in a secure manner; for instance, security could be provided using encryption tools.

With regards to identification of the data subject in video surveillance recordings, reasonable and necessary conduct from a credit institution would be to ask the data subject to clearly identify themselves in a specific video surveillance recording, to submit a photo of themselves or to describe their appearance (clothing and features etc.), and to state the data subject's exact location when recorded on video, as well as stating the time when the subject was recorded on video. If the information provided by the data subject is not sufficient for identification to be carried out, it is justified to ask the data subject to provide additional information to enable effective identification. In addition, while considering the issue of video recordings, one should evaluate whether the recording may be used to identify third parties, in which case protection of privacy of such third parties must be ensured by covering up images of them, or, if this not possible, considering the option of describing the circumstances under which they were featured in the relevant video recording.

[27] See also Section 5.1 of the Guidelines "Right to information".
[28] See: Peter Nowak vs. Data Protection Commissioner, Case C-434/16, 20.12.2017. judgement: http://curia.europa.eu/juris/document/document.jsf?-text=&docid=198059&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=635195
[29] See also Section 5.4 of the Guidelines "Right to data portability".

Regarding identifying the data subject in voice (audio) recordings, the data subject should, when requesting information about themselves, specify the probable time of their call, as well as their phone number (if the information is selected based on this phone number). While considering the issue of such a voice (audio) recording, the credit institution should also evaluate whether the voice (audio) recording contains data of the employee who communicated with the data subject. Thus, it would be expedient to determine the data subject's purpose of requesting the voice (audio) recording to determine whether the parts of the voice (audio) recording that contain the employee's statement should be issued or substituted with a written transcript of the essence of the conversation, and to evaluate whether the fulfilment of the purpose requires the identification of the employee of the credit institution who communicated with the data subject in the relevant voice (audio) recording.

For more information about the issues covered in this chapter – see Recitals 59, 61, 63, 64 and 73 GDPR, and Articles 12 and 15 GDPR.

5.3. Right to rectification

Essence of the right to rectification

The data subject is entitled to correct their data. A rectification request must be justified, and the credit institution should evaluate the substantiations. If the credit institution has doubts regarding the justifications for the request, it may ask that the data subject provide further evidence for the data rectification. However, it would not be appropriate to request additional evidence for rectification of data that are fully dependent on the data subject's discretion, such as a customer's place of residence, email address or phone number.

The credit institution is not obliged to rectify so-called subjective data – i.e. data or opinions created by the credit institution with regards to the data subject, such as the inclusion of the data subject in a specific risk category based on an assessment conducted by the credit institution; however, if the data subject does provide additional information that could affect the subjective data generated by the credit institution, the credit institution should review such data. As a result of the review, the credit institution is entitled, based on the nature of the additional data submitted, either to amend the subjective data or to leave the data unchanged. A similar situation may arise with regards to a subjective assessment of an employee performed by their manager – assuming that amending it lies within the area of responsibility of the manager or the employer.

Data rectification may be requested only with regards to facts provided by the data subject or legally obtained by the credit institution, such as names, financial indicators and job titles. With regards to a subjective assessment, the data subject may only request rectification of the fact of the existence of such an assessment, rather than of the content of the assessment itself.

In cases where the boundary between objective and subjective data is difficult to define (e.g. with regards to identifying a violation based on objective information (certain actions taken in committing the violation) and subjective information (an assessment of such actions)), the data subject should always be allowed to at least supplement the data with other information.

In practice, situations may arise where the right to rectification is exercised simultaneously with the right to restrict processing (pertaining to the accuracy of the data). Taking into account the interconnectedness of these rights, an appropriate procedure could be devised for processing the data subjects' requests, including the option to simultaneously exercise both rights.

Do sources of information need to be corrected?

The right to rectification should not be interpreted as the right to amend documents but as the right of the data subject to state that if any legal consequences result for the data subject, the appropriate corrected information should be used with regards to them.

For instance, if a customer indicates a particular phone number as their contact number on a customer questionnaire filled out in hard-copy form, then, upon exercising the right to rectification where the customer's phone number has been changed, the credit institution would not be obliged to correct the data in the document (which might affect the legal force of the document) but should rather ensure that the new phone number is used in further communication with the customer (e.g. by making the relevant modifications to the customer relationship management database).

One may therefore conclude that rectification is required once discrepancies in data are observed, and the consequences of the rectification would only affect subsequent data processing and decision-making.

One should pay special consideration to cases where a credit institution uses inaccurate data to make an inappropriate decision that requires revision in accordance with the provisions of the applicable legislation.

Data rectification within automated systems

Because the data subject's right to request data rectification also applies to data processing systems, such systems should implement the functionality for rectifying individual sets of data in a way that does not affect the operation of the entire system (e.g. errors in the system or system downtime as a consequence of rectification of information).

Furthermore, the GDPR entitles the data subject to supplement their data with additional information. Thus, the systems should include features for supplementing the information already available within the systems.

If the data subject wishes to rectify data generated by the credit institution (so-called subjective data): for example, their credit rating, the right to rectification applies to data entries (data used as the basis for automated processing and decision-making); in the event of data rectification, the data subject should have the right to request a review of the additional information generated by the credit institution on the basis of evaluating this data.

If a person is included in a certain category that reflects certain factors or abilities (for example, creditworthiness or credit risk), and the assessment is based on inaccurate facts (prior entries), this person is entitled to request rectification of the data on which the relevant assessment is based (i.e. information previously entered), and to review the assessment of the person based on this data.

Thus, automated systems must provide functionality for repeated processing based on rectified data.

Duties of the controller

Ensuring the accuracy of data is one of the fundamental duties of the credit institution in acting as the controller, since inaccurate data may lead to negative consequences for the data subject (e.g. information erroneously entered into a list of debtors which lowers creditworthiness indicators may mistakenly indicate to investigating authorities that the customer is involved in unusual and suspicious transactions); therefore, the credit institution must take various organisational measures to ensure data accuracy and regular updates, such as by including the customer's duty to immediately report changes to basic information in contracts, verifying that a customer's basic data are up-to-date while providing services to the customer in person, or periodically asking the customer via internet banking service to verify that their data are up-to-date.

Periods for the execution of requests

The credit institution reviews a request and, if necessary, adjusts the data without undue delay – and, no later than within one month after the receipt of the request, notifies the data subject about the actions taken. The period of time for executing a request, may be extended by up to 2 months, having taken into account the complexity and number of the requests. The data subject must be informed about the extension within one month following receipt of the request.

Should other data recipients be notified?

The credit institution should identify the data recipients to whom rectified data were disclosed prior to rectification and, unless this would require excessive effort (e.g. if difficulties finding information on data recipients render such identification technically complicated or expensive as compared to the benefit that would be derived by the data subject from such request), they should be notified about the execution of the rectification request. The credit institution should apply reasonable effort (i.e. use standard industry approaches to achieving the goal without necessarily using every tool available to the credit institution) to verify that the processors have appropriately implemented the data rectification request and subsequently processed the rectified data.

For more information about the issues covered in this chapter – see Recital 73 GDPR; and Articles 12 and 16 GDPR.

5.4. Right to data portability

Essence of the right to data portability

The data subject is entitled to receive their data to preserve, or to reuse them, e.g. by transferring them to another service provider. In terms of the amount of data processed, this right is different from the right of access, where the amount of data to which a data subject can have access is much greater.

To what data does the right to portability apply?

The right to data portability is not absolute; it only refers to a certain range of data. The data must match the following criteria to be subject to the right to portability:

1. **the data relate to the specific data subject who submitted the application:**

   a) including pseudonymised data (but not anonymous data, which cannot be connected to a specific person)

   b) the evaluation of issued data must verify that the transfer of data will not affect other persons' rights to data protection

2. **data provided to the credit institution by the data subject him-/herself:**

   a) there are not exclusively the data provided by the data subject by e.g. filling out online application forms, but also data arising during the course of the monitoring of the data subject's activities (e.g. website browsing history, location data or data from "smart devices")

   b) there are not the data created by the credit institution itself (e.g. evaluation of the credit risk of the customer created by the credit institution, or the assignment of the customer to some group such as professional/non-professional customer, would be considered data generated by the credit institution and will not be subject to the right to data portability)

3. **refers only to data which are processed on the legal basis of the consent of the data subject, or the necessity of performing a contract (including drafting a contract) to which the data subject is party**

   a) portability applies to information about the customer's transactions made to/from the account or digital applications submitted by the customer for various products (e.g. products carrying credit risk)

   b) portability does not apply to information collected in order to comply with the AML/CFT Law, or information collected independently by the company in the context of assessing the customer's creditworthiness

4. **the processing of such information is performed by automated means**, i.e. the credit institution does not need to ensure the portability of information recorded on paper.

Thus, the credit institution's systems should implement the option of selecting or otherwise flagging the relevant data categories, so that the data subject's information which is subject to the right to data portability can be effectively selected and exported if the data subject so requests.

It is recommended to choose a solution that would allow the data subject to ensure the portability of certain pieces of information, rather than the entirety of the information, thereby allowing the data subject to select the appropriate amount of portable information.

The Article 29 Working Party has stated its opinion[30] that information subject to data portability may contain the data of third parties, which does not impede portability in and of itself, although the impact of transferring such data on the rights and freedoms of third parties should be taken into account. If an unfavourable impact is likely, measures should be taken in order to, as far as possible, prevent such unfavourable consequences.

Should data accuracy be evaluated while data are being prepared for portability?

The implementation of the right to data portability applies to information that is at the credit institution's disposal; the credit institution is not specifically obliged to verify data prior to sending.

Do the data that are sent need to be deleted upon sending?

Sending the data does not mean that the right to process the data in the context of existing legal bases and for previously specified purposes is now void; thus, sending of the data does not require deletion of the data.

Data sending format

Data should be sent in a structured, commonly used, machine-readable format (thus allowing software to easily identify, distinguish and extract data, as well as to recognise the internal structure of the data) that is suitable for reuse. The GDPR does not specify a definitive format or structure for data, and allows for each industry to have different types and structures of data, and therefore creating a uniform approach could be a future initiative for the industry.

Examples of interoperable open file formats usable by different systems include *.xml un *.csv formats.[31] The transfer of data should include the metadata that the data recipient requires to reuse the data.

[30] Article 29 Working Party "Guidelines on the right to data portability" as of 13 December 2016, page 11: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[31] Ibid., page 17.

How and to whom should the data be transferred?

At the data subject's discretion, data should be sent to the data subject themselves (subject to the identification provisions listed in the section of this document on the right of access) or to the service provider they specify. However, if the data are sent directly to another service provider, the credit institution should send the data using secure means agreed upon by both of the parties. The security of the data must be ensured both for the transmission process (using, for example, end-to-end encryption) and for the recipient (using a stringent process of identification and authentication).[32] However, these activities should not excessively impede the implementation of portability (e.g. by specifying a fee, except in the cases listed below). The data subject must be made aware, and preferably the credit institution should notify them, that transmission of information will entail the provision of the data to a third party, potentially disclosing the customer's secrets.

Tools are recommended to implement automatic data downloading (ensured via most internet banking systems' account statement functionality), or to provide some other way for the data subject to send the data directly to another service provider, using, for example, the aforementioned internet banking solutions.

If the data are transferred to the data subject, the data subject should be informed about how to store the data securely, because it is highly probable that the data held at the customer's disposal will be less well protected compared to the data held in the credit institution's systems.

Obligations for the credit institution upon receiving such data

If the customer sends the data to the credit institution as a result of implementing their right to data portability, the credit institution should specify the minimum amount of data necessary to provide the relevant service. If, within the framework of such rights, the credit institution receives more information than it needs to provide its services, it should delete the excessive information or, if this is impossible due to the nature of the information and its relation to the data subject, this information should not be used for other purposes except those stated by the customer/data subject.

Periods for the execution of requests

The credit institution executes the transfer without undue delay – and, in any case, within one month of receipt of the request, notifies the data subject about the actions taken. The period of time available for execution of the request may be extended by up to 2 months, having taken into account the complexity and number of the requests. The data subject should be informed about the extension of this period within one month of receipt of their request.

Accountability

Controllers that have executed a request for data portability are not accountable for subsequent processing performed by the data subject or by another person that receives the data.

For more information about the issues covered in this chapter – see Recitals 68 and 73 GDPR; and Articles 12 and 20 GDPR, as well as the Article 29 Data Protection Working Party recommendations of 13 December 2016, "Guidelines on the right to data portability".

[32] Article 29 Working Party "Guidelines on the right to data portability" as of 13 December 2016, page 16: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

5.5. Right to erasure ('right to be forgotten')

Essence of the right to erasure ('right to be forgotten')

The data subject has the right to demand that the credit institution, without undue delay, deletes the data subject's data, and the credit institution is obliged to delete the data without undue delay if:

1. the data are no longer necessary or useful in relation to the initial purposes for which they were collected or otherwise processed (e.g. the data subject may request erasure of the data in a situation where the credit institution collected the data for a lottery, if the lottery has taken place, and the data are no longer useful for the initial purpose)

2. the data subject has withdrawn the consent on the basis of which the data processing was carried out, and there is no other legal basis for the processing (however, one should evaluate whether evidence of the lawfulness of data processing during the effective period of consent needs to be stored within the framework of the credit institution's legitimate interests)

3. the data subject has objected to the data processing and, following repeated assessments of the legitimate interests, the credit institution finds that the data processing has no legal basis, or processing takes place for marketing purposes (e.g. the data subject may have data deleted if the credit institution uses the data solely for advertising or as part of a marketing campaign)

4. the data have been processed unlawfully (e.g. the credit institution has failed to comply with the requirements of the GDPR regarding observance of the lawfulness principle in processing the data)

5. the data must be deleted because this is specified in the legislation applicable to the credit institution

6. the data were collected in connection with the offering of information society services to a child on the basis of consent (e.g. the data subject may request erasure of the data in a situation if the credit institution collected the data subject's data at a time when the data subject was a child, regardless of whether the data subject or person having parental responsibility for the child provided consent at the time)

Periods for the execution of requests

The credit institution deletes information without undue delay – and, in any case, within one month of receipt of the request notifies the data subject about the actions taken. The period of time available for execution of the request may be extended by up to 2 months, having taken into account the complexity and number of requests.

Examples of cases when the erasure of data must not be performed

Data may be retained without considering other circumstances in the following cases:

1. to exercise the right of freedom of expression and information

2. to comply with a legal obligation requiring data processing (e.g. the periods for information or document retention specified in the applicable legislation, such as the AML/CFT Law, the law On Accounting or the Credit Institutions Law)

3. to perform a task carried out in the public interest or in exercising the official authority vested in the controller (for example, if a credit institution proves that the wider public needs access to the particular data, and that this information is sufficient, substantial and adequate to the purpose)

4. on the grounds of public interest in the area of public health;

5. if the processing is necessary for the purpose of archiving in the public interest; for the purposes of scientific or historical research; or for statistical purposes, provided that the aforementioned rights could prevent or substantially impair the fulfilment of the purposes of such processing.

Can the data processing be replaced by data anonymisation?

If the information systems solution implemented at the credit institution does not support the complete erasure of data fields or a person's profile, and the erasure of data or a customer's profile could threaten the functionality of the system, the alternative is to anonymise the data, i.e. to delete all identifiers (data fields) based on which a person might be recognised, namely, by anonymising the data. In terms of legal consequences, the anonymisation process is equivalent to data erasure.

Likewise, the anonymisation method may be considered in cases where statistical indicators require the preserving of customers' prior habits of service use, in such a way that, provided that all personal identifiers are deleted, the person may no longer be considered identifiable and the remaining data can no longer be treated as personal data. However, when anonymising data, one should carefully select the anonymisation methods so that the credit institution is certain that the remaining information cannot be used for recognising and identifying the person, and that the anonymisation process has irreversibly erased the data entered. Details on anonymisation methods and the ways in which data can be de-anonymised are provided in the Article 29 Working Party "Opinion 05/2014 on anonymisation techniques" as of 10 April 2014.[34]

Do other data recipients need to be informed?

The credit institution should identify data recipients to whom the data has been disclosed, and, they should also be notified about the execution of the request of such person, unless this requires excessive effort (e.g. if difficulties finding information on data recipients render such identification technically complicated or expensive as compared to the benefit derived by the data subject from such a request). The credit institution should apply reasonable effort (e.g. use standard industry approaches to achieving the goal, without necessarily using every tool available to the credit institution) in order to verify that the processors have appropriately implemented the request for data erasure.

For more information about the issues covered in this chapter – see Recitals 65, 66 and 73 GDPR; and Articles 12, 17 and 19 GDPR.

5.6. Right to restrict processing

Essence of the right to restrict processing

The data subject is entitled to request that the credit institution restricts processing, i.e. labels the personal data to restrict processing in the future. The data subject is entitled to demand that the credit institution limits processing if any of the reasons specified in the following table apply.

[34] Article 29 Working Party "Opinion 05/2014 on anonymisation techniques" as of 10 April 2014: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Table No. 6

Reasons for restriction of data processing

Reason	Duration of restriction
1. the accuracy of the data is contested by the data subject	For a period enabling the credit institution to verify the accuracy of the data (except in cases where the credit institution must follow the periods for fulfilling obligations as stated in the applicable legislation)
2. the processing is unlawful and the data subject opposes the erasure of the data, requesting the restriction of its use instead	For the period requested by the data subject, if the period specified by the data subject is justified
3. the credit institution no longer needs the data for the purposes of processing, but it is required by the data subject for the establishment, exercise or defence of legal claims	For the period requested and justified by the data subject
4. the data subject has objected to processing that is based on the legitimate interests of the credit institution (or task carried our in public interest)	For a period sufficient to enable verification of whether the legitimate interests of the controller override those of the data subject

It should be considered that, the data subject's objections to processing may be received at the same time that a data processing restriction request is made. Such requests should be considered with reference to the rights to object to data processing as specified in Section 5.7 of the Guidelines.

Methods for implementing restriction

Data processing may be restricted in various ways: by transferring the relevant data to another processing system; by setting a restriction on users accessing the relevant data within the system; by recalling/removing published/transferred data from the location where it has been published; by disabling the restricted data within the automated systems that use it; by restricting the options for modifying it, and by inserting a note within the system stating that the data are restricted; or by performing other activities, if necessary.

It follows from the aforementioned arguments that the feature sets of systems must provide the opportunity to select certain categories of a specific data subject's data with regards to which processing is restricted, thus allowing for the implementation of the aforementioned methods for restricting processing. Furthermore, the automated systems must prevent the disruption of system operations due to the processing restrictions.

A problem may arise where the same data are being used for various purposes but the restriction only applies to one of these purposes. A solution in this situation would be to flag the data to indicate what purposes data processing is restricted for.

What are the rights to process data if the data subject has restricted data processing?

Accordingly, the data may only be stored, and not processed once a restriction has been set; any such data, with the exception of storage, may only be processed with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the EU or of a member state.

In accordance with the GDPR, the credit institution should evaluate each case individually, so that, once a restriction has been set, only data storage is performed, or storage is accompanied by data processing in other ways.

Request execution periods

The credit institution restricts the use of data without undue delay – and, in any case, within one month following receipt of the request, notifies the data subject about the actions taken. The period of time available for execution of the request may be extended by up to 2 months, having taken into account the complexity and the number of the requests. The data subject should be informed about the extension of this period within one month of receipt of their request.

Notifying the data subject

Before removing restrictions, the credit institution should notify the data subject.

Notifying other parties

The GDPR also specifies that each recipient of the data (whether external or internal) must be made aware of the processing restrictions, so that they have information about such restriction and can accordingly comply with that. Thus, the relevant data recipients must be established and registered, and notified accordingly about applicable data processing regimes. For instance, if a processing restriction applies to information regarding the debt reported to a credit information bureau, the credit institution should notify the relevant credit information bureau; otherwise, third parties will continue to collect information that has been restricted (e.g. regarding a dispute concerning the data accuracy) and make decisions affecting the data subject based on such possibly inaccurate information.

For more information about the issues covered in this chapter – see Recitals 67 and 73 GDPR; and Articles 12, 18 and 19 GDPR.

5.7. Right to object

Essence of the right to object

The data subject is entitled to object to the processing of their data in the cases listed in the table below.

Table No. 7

Grounds and consequences of an objection to data processing

Basis for implementing the right to object	Consequences of objection
Where processing is based on the legitimate interests of the credit institution (Article 6(1)(e) GDPR) or the interests of the public and performance of a task carried out in the public interest (Article 6(1)(f) GDPR), including profiling based on those provisions.	Upon receiving a person's request containing specific reasons related to the data subject's particular situation, the credit institution should no longer process the data for certain purposes, unless the credit institution: 1) 1) is able to demonstrate compelling legitimate grounds for the processing that are the basis for continuing data processing despite the interests, rights and freedoms of the data subject (including the review of the interest balancing result for the specific processing activity) 2) uses the data for the establishment, exercise or defence of legal claims. If the data subject has also indicated a restriction of data processing, then, until the request has been reviewed, the data must be no longer processed until the credit institution is found to have a reason to carry on with the processing.

Processing required for the purposes of direct marketing, including profiling.	Upon receiving objections to processing, the credit institution shall no longer process the data for the relevant purpose.
Processing performed for scientific or historical research purposes or statistical purposes	Upon receiving objections, the credit institution shall no longer process the data for the relevant purpose, unless such processing is required to perform a task carried out for reasons of public interest.

The right to object may not be exercised by the data subject if the basis for the data processing is:

1) consent
2) the establishment and performance of contractual relationship
3) the execution of a legal obligation
4) the protection of vital interests of the data subject or third parties.

Periods for the execution of requests

The credit institution reviews a request and ceases data processing without undue delay – and, in any case, within one month following receipt of the request, notifies the data subject about the actions taken. The period of time available for execution of the request may be extended by up to 2 months, having taken into account the complexity and number of requests. The data subject should be informed about the extension of this period within one month of receipt of their request.

For more information about the issues covered in this chapter – see Recitals 69, 70, 71 and 73 GDPR; and Articles 12 and 21 GDPR.

5.8. Rights with regards to automated individual decision-making

Automated individual decision

An automated individual decision is a decision based solely on automated processing, which produces legal effects concerning the data subject or similarly significantly affects the data subject. Automated individual decision-making may take place with or without profiling.

Profiling

Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

It follows from the GDPR that profiling is an automated form of data processing that allows for the analysis of available data, monitoring behaviour and making forecasts pertaining to the data subject.

For instance, profiling is performed at credit institutions as part of processes necessary for granting a loan and specifying the lending terms, granting a consumer loan, and identifying suspicious transactions.

Three key means of using profiling may be identified:

1) general profiling which does not lead to individual decisions being made
2) profiling as a result of which an individual decision is made with human intervention
3) automated individual decision-making, including profiling.

As a result of profiling, a decision may be based on automated processing, while in case "c", the decision is made by an algorithm without any meaningful human input.

The right of the data subject under Article 22 GDPR only refers to an automated individual decision (including profiling), without human intervention in the decision-making process or without any meaningful human input, and which produces legal effects for the data subject or similarly affects the data subject.

Significance of the automated decision-making

Automated decision-making, including profiling, may produce legal effects for the data subject (including negative consequences) or otherwise significantly affect the data subject [e.g. in cases of the automatic refusal of an online credit application, or the assignment of an increased interest rate (within the boundaries specified by law) as a result of the credit application, without rejecting it outright]. Thus, the data subject must be informed that the received data will be used for automated decision-making (including profiling) and should be able to control the making of such decisions with reference to them.

Although in some cases individualised marketing (which is generally based on profiling) may also produce significant effects, in most cases where such an individualised marketing approach is applied to a very broad category of persons (e.g. customers who have an account with a bank but do not hold any payment cards or credit cards), it may be assumed that such profiling does not produce significant effects for the data subject.

The GDPR entitles the data subject to receive a meaningful report/information on the envisaged processing and the logic involved in the processing (to an extent that does not infringe the substantial interests of the credit institution – for example, by disclosure of a trade secret or infringement of intellectual property – and does not cause other substantial risks to the interests of the credit institution) if automated decision-making (including profiling) takes place. Appropriate measures should be taken to provide the data subject with such information in a concise, transparent and easily accessible form, using clear and plain language, and to maintain communication with the data subject with regard to the processing. The information is provided in writing or by other means (including by electronic means).

As an example of profiling would concern the inclusion of a customer in a category of customers based on a marketing strategy selected by the credit institution that groups customers by age (for instance, to avoid offering loans to customers under the age of 18, or to offer specific products to students and to young people under the age of 25), who are provided with some customised products or services of the credit institution.

The right to refuse

The data subject has the right not to be subject to an automated individual decision, including profiling, if all the following criteria are met:

1) the decision is based solely on automated processing, including profiling, and
2) the decision produces legal effects for the data subject or similarly affects the data subject.

The data subject is entitled to obtain human intervention in automated decision-making if it produces legal effects for the data subjects or similarly affects them in order for the data subject to express his or her point of view and to contest the decision. The relevant person must have the competence and authority to revise an automated decision. In order to confirm human intervention in decision-making, one should ensure careful oversight of the decision by a competent and authorised person considering all the available data on which the decision is based. An example of this would be a recommendation for a decision developed by an automatic process that refers to the data subject. If a human reviews this decision and takes into account other reasons for the decision that was ultimately made, the human is considered to be involved in the decision-making.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 May 218, the Data State Inspectorate expressed the opinion that for automated creditworthiness checks resulting in automated individual decisions regarding the data subject the provisions of Article 22(3) GDPR apply – i.e. the credit institution shall ensure to the data subject the right to contest the adopted decision and request revision thereof, by ensuring participation of the credit institution's staff in the decision-making.

Exceptions

The data subject is not entitled to refuse automated individual decision-making if a decision:

1. is necessary for entering into or performance of a contract between the data subject and the credit institution (e.g. automated monitoring of payments, automatic review of information stated in a payment order or a request to review one's payment order if the information is inconsistent) – in such cases, the credit institution should ensure human intervention in decision-making so that the data subject is able to express their point of view and contest the decision

2. is authorised by the EU or Latvian law to which the credit institution is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests (e.g. customer due diligence; or maintenance of systems for detection of unusual and suspicious transactions, for compliance with the AML/CFT Law)

3. is based on explicit consent from the data subject – in such cases, the credit institution should ensure human intervention in decision-making so that the data subject is able to express their point of view and contest the decision.

Periods for the execution of requests

The credit institution reviews a request without undue delay and, in any event, within one month of receipt of the request, notifies the data subject about the activities performed. The period of time available for execution of the request may be extended by up to 2 months, having taken into account the complexity and number of requests.

For more information about the issues covered in this chapter – see Recitals 60, 71, 72 and 73 GDPR; and Articles 12 and 22 GDPR, as well as the Article 29 Working Party "Guidelines on Automated individual decision-making and Profiling for the purposes of GDPR 2016/679" as of 3 October 2017 [35].

[35] Article 29 Working Party "Guidelines on Automated individual decision-making and Profiling for the purposes of GDPR 2016/679" as of 3 October 2017: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

6. TECHNICAL AND ORGANISATIONAL MEASURES FOR COMPLIANCE

6.1. Key requirements for internal policies

While the GDPR does not specify that any documents in particular are necessary to maintain, with the exception of the data processing register, good management principles for accountability and transparency would include the documentation of personal data processing to clearly reflect the compliance of credit institutions' activity with the GDPR.

Personal data protection procedures and requirements in accordance with the GDPR may be included in existing internal documents by updating them or specified in new documents that specifically focus on data processing.

In the context of accountability, the clearest way to demonstrate compliance with personal data protection requirements would be to develop a separate personal data protection policy document that would set out general principles for data protection, the staff responsible for implementing the policy and specific personal data processing procedures – including references to other internal regulations.

For instance, the personal data protection policy specifies a general principle for collecting personal data in the amount necessary for fulfilment of a specific purpose, but a reference to the anti-money laundering and counter-terrorist financing policy is provided which specifies the scope of personal data collected and includes criteria based on which one may determine whether the collected information is sufficient for complying with the relevant anti-money laundering and counter-terrorist financing requirements.

One should consider the development of internal procedures, in addition to the existing ones that entail compliance with the Financial and Capital Markets Commission's normative regulations No. 112 "Normative regulations for the security of finance and capital market participants' information systems" as of 7 July 2015, which refer to the following personal data protection areas and aspects:

1) policy for the protection of personal data

2) processing of customers' personal data:
- privacy policy
- privacy announcements and clauses, consent
- use of data for marketing purposes
- cookies and online activity monitoring

3) human resources management and safety:
- notification of employees and candidates, processing of their personal data
- monitoring of employee devices, and their activities on the internet and elsewhere, including access to employees' files and communications (may be integrated into internal security policy)
- video surveillance
- operation of a whistle-blower scheme
- staff training

4) processing of the personal data of suppliers and business partners

5) review and execution of data subject requests

6) involvement of other parties in data processing:
- forwarding data to other controllers [includes the regulation of joint controller relationship (e.g. liability)]
- processor access to data (e.g. requirements for processor contracts, monitoring processes, cloud computing policy) – may be integrated in outsourcing policy
- forwarding data outside the EU or to international organisations
- receiving data from third parties (e.g. external databases)

7) ensurance of accountability:
- maintenance of the data processing register
- activities of a data protection officer
- procedure for performing a data protection impact assessment
- procedure for evaluating legitimate interests

8) technical and organisational requirements (may be integrated into the information security policy):
- an anonymisation and pseudonymisation procedure
- data encryption and access restrictions
- plan for remedying personal data breaches

9) procedures for storage, archiving and destruction of personal data (may be integrated into the accounting procedure)

10) job description for a data protection officer

11) personal data breaches:
- response, reporting of personal data breaches
- a register of personal data breaches
- a template for reporting a personal data breach to the supervisory authority
- a template for reporting a personal data breach to data subjects.

For more information about the issues covered in this chapter – see Recital 74 GDPR; and Articles 24, 29 and 32 GDPR.

6.2. Keeping internal records of processing activities

Should the credit institution create a register of processing activities?

The credit institution should maintain at least a register of its processing activities in the controller role. Maintenance of a register of personal data processing activities is recommended as a means of implementing the accountability principle. It is not necessary for a register of processing activities to be created if the credit institution employs fewer than 250 persons and its processing would not result in a risk to the rights and freedoms of data subjects, if the processing is not occasional , and if the processing does not include Special Category of data or data relating to criminal convictions and offences. In practice, credit institutions are only in very rare cases permitted not to maintain a register of processing activities.

The register of processing activities should also include a description of the processing activities performed at a credit institution's branches. The register should be maintained as clearly as possible, to render it intelligible not only to persons maintaining the relevant register but also to other persons who require access to the register of processing register, e.g. to clarify data processing procedures and purposes for the data subject.

If the credit institution operates as a data processor having been assigned the role by other controllers, the credit institution should also maintain a register of the processor's (i.e. the credit institution's) data processing activity categories.

Maintenance of a data processing register should be entrusted to a person that has access to information regarding all processing activities taking place within the credit institution, and exchange of information regarding any changes to processing activities must be ensured to allow accurate recording in the current version of the register of processing activities.

The maintenance process of the register of processing activities may involve the data protection officer, within their area of responsibility (e.g. in order to evaluate whether the purpose of data processing has been defined appropriately).

Table No. 8

What information should be included in the registers?

Recorded information	Register of activities of the credit institution in acting as the controller	Register of categories of processing activities of the credit institution in acting as the processor
Name and contact information (address, phone number, email address) **of the credit institution** (including joint controllers[36]).	✓	
Name and contact information (address, phone number, email address) of the processor.		✓
Company and contact information (address, phone number, email address) **of the controller** (their representative) **on behalf of whom the credit institution operates as a processor.**		✓
First name, surname and contact information of the data protection officer (e.g. provided at the credit institution's discretion, an address where the data protection officer may be reached, or an email address that allows communication with the data protection officer).	✓	✓
Processing purposes (e.g. provision of services to customers, identification of the ultimate beneficial owner, transaction monitoring for the purposes of compliance with the AML/CFT Law, monitoring of applicants' creditworthiness)	✓	
Description of data categories (e.g. identification data, financial data etc.)	✓	✓
Description of data subject categories (e.g. customers, ultimate beneficial owners, employees, persons within the area of video surveillance, payment beneficiaries, visitors).	✓	
Categories of processing carried out on behalf of each controller		✓
Categories of data recipients to whom data have been or will be disclosed (e.g. courts, service providers, public authorities)	✓	
Information on transfers of data to a third country or international organisation, identification of such countries and organisations, documentation of safeguards, if the data are transferred under circumstances specified in Article 49(1)(2) GDPR (e.g. types of data sent and legal bases)	✓	✓
Where possible – envisaged time limits for erasure of different categories of data	✓	
Where possible – general description of technical and organisational security measures (specifying, for example, how data are protected against the risks of physical impact, unintentional deletion, cyber-attacks; or specifying such information in another related document)	✓	✓

[36] In accordance with Article 26 GDPR, "where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".

In what form should the register be maintained?

The register should be maintained in writing. Electronic form is recommended to ensure that information is conveniently and easily accessible.

The following is an example of a register (assuming that the general description of technical and organisational security measures is maintained separately), which can be adjusted to take into account the specifics of activities at the relevant credit institution.

Table No. 9

Template of register sections

Controller name	Data protection officer	Purposes of processing	Categories of data	Data subject categories	Categories of data recipients	Information on transfers of data to a third country	Retention period
SIA "BANK", bank@bank.eu, ph.: 27654321	Jānis Pēteris janis@bank.eu,	Employee recruitment	Identification data, financial data	Employees	Public authorities	No data sent	5 years
		Protection of own property	Location data, biometric data	Persons within the area of video surveillance	Service providers, public authorities	No data transfer	2 weeks

Register updates

Taking into account that the business environment is variable and new services are being created, new regulatory requirements introduced, and existing ones amended, it must be ensured that the register is updated regularly. To ensure this, a responsible person should be assigned to be in charge of maintaining the register.

Is the register subject to disclosure?

The register must be made available to the supervisory authority upon request.

For more information about the issues covered in this chapter – see Article 30 GDPR.

6.3. Data protection impact assessment

Purpose, essence of assessment, relation to other processes

A data protection impact assessment (DPIA) is intended to identify and mitigate risks, to facilitate the introduction of adequate data protection solutions, and to prevent the loss of reputation and trust.

Credit institutions currently have in place a variety of approaches to carrying out a DPIA – in some cases, no separate DPIA is carried out; in others, data protection aspects are included in an overall process of risk assessment (as part of compliance risk); also, some credit institutions may have separate procedures specified, and special committees created to conduct the DPIA. In connection with other processes for risk management, aspects of DPIA at credit institutions may be included in the compliance risk assessment procedure, or in the business impact assessment procedure.

Importantly, the GDPR only provides for an assessment in terms of data protection. Privacy risks is a broader concept, and the management of privacy risks can include other actions, for example, the protection of communication privacy (which may or may not contain personal data), including data protection, and situations may arise where privacy risks are not related to aspects of data protection at all.

Taking it into account, the DPIA process may need to be harmonised with existing processes to ensure privacy and information security risk management. In essence, the DPIA is part of the risk management process. Thus, depending on an evaluation of the needs and the internal organisation of each credit institution, the DPIA may be either included in the existing risk management processes to make this element compliant with the GDPR, or placed in a separate procedure.

In order to fully comply with the provisions of the GDPR regarding the necessity of the assessment, and how the procedure should be carried out, it is advisable to include a requirement to evaluate the existence of data processing – and the degree of a risk that such processing poses to rights and freedoms of natural persons in the context of data protection – within the existing compliance, information security and privacy risk management process (depending on the needs of each credit institution). Thus, upon the identification of a high risk (based on the criteria specified in the GDPR and considering the operational specifics of a given credit institution), one might commence a separate DPIA – thereby fulfilling the requirements of the GDPR.

The DPIA should be a continuous procedure throughout the processing (from commencing data processing until data erasure) rather than a separate assignment resulting in a statement.[37] Thus, the DPIA should be integrated with risk management processes to ensure continuous operational risk assessment in the context of data protection.

When should a DPIA be performed?

A DPIA is mandatory if the processing is likely to result in a high risk to rights and freedoms of natural persons. High risk may result from the type of processing, the technologies used, the nature of processing, the scope of the processing, the context of the processing, or the purposes of the processing. The DPIA should be documented in order to prove that the requirement has been fulfilled in compliance with the GDPR.

The existence of a high risk to rights and freedoms of natural persons is established, and a DPIA should be carried out, in at least the following cases (this list is not exhaustive):

1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or significantly affect the natural person.

   For instance, most credit institution services are related to systematic, large-scale evaluation of data subjects, e.g. assessment of creditworthiness or monitoring of customer payment obligations.

2. processing on a large scale of Special Categories of data, or of personal data relating to criminal convictions and offences.

   For instance, processing of data of a credit institution employee in connection with criminal convictions and offences, and processing of Special Category of data, in order to verify that the employee is suitable for the position held, or to ensure performance of the contract, is not considered data processing on a large scale, although, if customer data or Special Category of data are processed as part of providing services, this may be considered a data processing on a large scale.

[37] See also: https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf

3. systematic monitoring of a publicly accessible area on a large scale, such as using video surveillance.

The Article 29 Working Party has stated in its guidelines a list of criteria that may indicate the existence of a high risk in the context of data processing (the risk is higher if more criteria are met by the data processing), and these are listed in the table below.

Table No. 10

Criteria for high-risk data processing

Criterion	Description
Profiling or other assessment of personal aspects of data subjects	For example, if the credit institution evaluates customers' creditworthiness or fraud risks, particularly if the information is used to make decisions binding upon the data subject (e.g. refusal to provide service).
Automated decision-making that may produce legal effects or other significant consequences for the data subject	For example, the credit institution identifies fraud risks using automated tools and automatically forwards this information to the security services or law enforcement institutions, or the credit institution evaluates a customer's application and makes an automated decision to approve or deny a loan.
Continuous or systematic monitoring of data subjects	This criterion is especially crucial in cases where the data subject is not sufficiently informed about data processing (regarding whether data are processed, who processes the data, and for what purpose the processing is performed), and in cases where the data subject is unable to avoid such data processing, e.g. in public spaces.
Processing of Special Category of data	For instance, if the credit institution determines a customer's ethnicity or introduces biometric access control systems on the premises of the credit institution.
Data processing on a large scale	If a substantial part of the customer base is subject to processing, this would be considered a processing on a large scale.
Merging of datasets	For example, the credit institution decides that, in order to provide services more effectively, it will merge its customer dataset with a publicly available dataset so that, for example, changes to customers' lifestyles (solvency data) are recorded automatically.
Data processing will apply to vulnerable data subjects	For example, processing the data of children, seniors, or employees.
Use of new technologies or software	The use of new technologies or software – for example, to introduce a facial recognition system, or identify whether a person might present a fraud risk – always involves unknown risks that the relevant solutions may affect the right of the data subject to the protection of their data; thus, the use of any new technological or software solutions should involve an evaluation of whether a DPIA is necessary.

The Article 29 Working Party recommends[38] that, if at least two of the aforementioned criteria are applicable to data processing, a DPIA is recommended, although cases where a single criterion would be sufficient cannot be excluded.

For instance, a DPIA is necessary in cases where the credit institution, in order to manage customer credit risk, obtains and preserves data from publicly available sources and other databases – such processing would require a DPIA because it involves three of the aforementioned criteria: (1) assessment of personal aspects of the data subject; (2) merging of datasets; and (3) data processing on a large scale.

The nature of a credit institution's activity is that its everyday processing of customers' data qualifies as a processing on a scale, which is one of the criteria for high-risk processing; however, while evaluating risks, one should also take into account the high degree of regulation of credit institutions or specified minimum information security requirements that might be a justified argument for mitigating risks.

[38] Article 29 Working Party "Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" as of 4 April 2017, page 11.

The Article 29 Working Party guidelines highlight the processing on a large scale as being a criterion for high-risk processing. Based on the examples stated in the Article 29 Working Party guidelines regarding data protection officers[39], the processing of customer data in the regular course of business of a credit institution could be considered a large-scale processing. Thus, nearly all data processing activities by a credit institution involving customer service exhibit a criterion for high-risk processing.

On the other hand, everyday customer service procedures at credit institutions are strictly regulated, controlled and well-understood, rendering it unjustified to assume that all customer data processing by a credit institution results in a high risk to data subjects just because it is large-scale, and thus requiring a prior DPIA for such processing. The deciding factor for determining the necessity of a DPIA should be a statement regarding the overall processing risk, rather than only taking into account individual criteria.

Supervisory authorities are also obliged to publish a list of processing activities that require a DPIA, although it should be taken into account that the list is subject to change. The list was approved by the Data State Inspectorate on 18 December 2018.[40] Thus, in cases where a credit institution considers the published list of processing activities and decides not to carry out a DPIA based on its assessment of processing risks, one should conduct ongoing tests of whether the relevant processing is included on the list developed by the supervisory authority.

In the event of cross-border processing, the lead supervisory authority's published list should be consulted. If the controller suspects that the relevant processing might be included on the list created by the supervisory authority of another member state where the processing will be performed, it should consult with the lead supervisory authority to determine the necessity of a DPIA, including the cooperation mechanism.

If the credit institution is unsure about whether a DPIA is required, a DPIA is recommended as an effective mechanism for ensuring GDPR compliance. Consulting with the supervisory authority is also an option, if necessary. During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that the DPIA should be treated as a dual tool. On the one hand, there are sanctions imposed for failure to perform the DPIA, on the other hand, DPIA helps the data controller to retain control over internal proceedings and systematize them. Therewith, the DSI urges not to treat the DPIA as a formal legal requirement.

Cases where a DPIA is not necessary

It is not necessary to carry out a DPIA if the technical basis for the processing is the execution of a legal obligation or the exercising of official authority vested in the controller (point (c) and (e) of Article 6(1) GDPR); for example, credit institutions complying with the AML/CFT Law will not need to conduct a DPIA on the basis of requirement by law, but with regard to creditworthiness review, the DPIA would probably be necessary because, even though the Consumer Rights Protection Law specifies the obligation of verifying a customer's creditworthiness, in addition to the requirement specified in the law, the credit institution also has legitimate interests of its own (avoiding losses), and thus it selects the creditworthiness assessment tools independently while conducting a higher amount of data processing than the legally mandated minimum. Similarly, a DPIA will not be necessary if the context, scope and purposes of intended processing are similar to a processing for which a DPIA has already been carried out.[41]

Supervisory authorities are entitled to specify and publish a list of processing activities that do not require a DPIA; thus, credit institutions should keep track of the content of such a list and any changes to it.

[39] Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')" as of 13 December 2016, page 8, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100.
[40] See: LV-DPA, Types of processing operations which are subject to the requirement for a data protection impact assessment according to Article 35(4) GDPR: https://www.dvi.gov.lv/lv/media/92/download (in Latvian).
[41] See also Section 6.3 of the Guidelines "Data protection impact assessments" on "Collaborative and joint impact assessment".

Assessment of data processing activities commenced prior to 25 May 2018

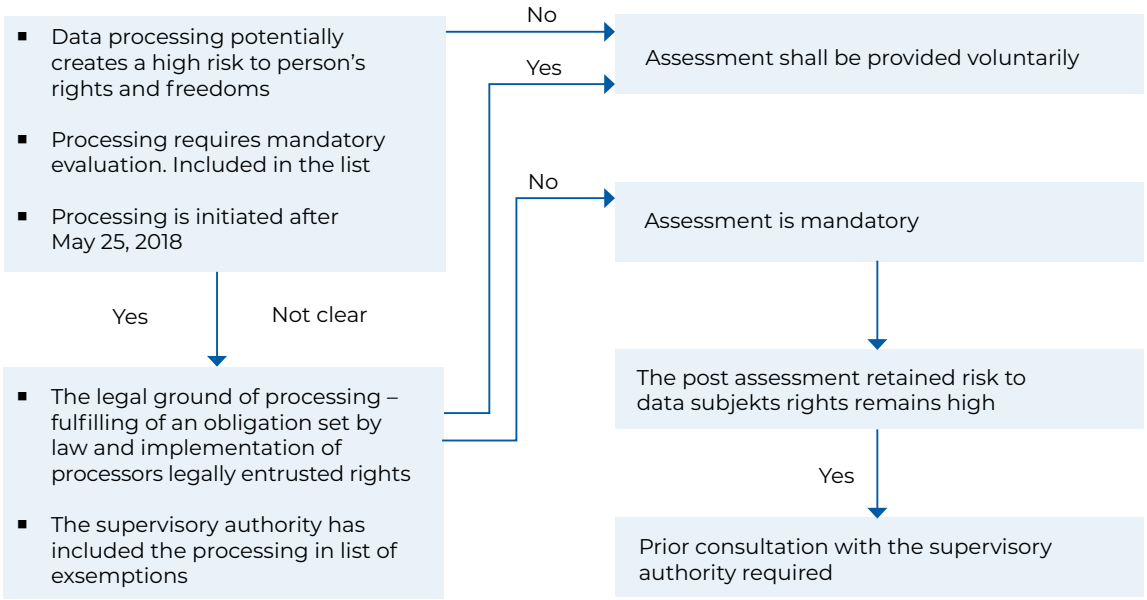
The duty to conduct a DPIA applies to processing activities commenced post 25 May 2018. Although the GDPR does not specifically indicate whether a DPIA is necessary once the GDPR is applied, if any substantial changes to a processing activity take place, or the risks of the processing change significantly (e.g. technological changes or amendments to regulations), a DPIA is necessary. During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate recommended not to wait for the expiration of the current term for revising the purposes of processing. Although the DSI could treat the ongoing monitoring as a good practice, the DSI considers that the data controller may not rely solely on regular purpose/process revision routines and after 25 May 2018 it is necessary to verify whether the processing does not involve any actions that do not correspond to the previously registered purposes (high-level purposes) or fall beyond them.

Thus, the recommendation is to conduct a DPIA of high-risk processing activities commenced before the GDPR became applicable, in order to identify and avoid any data protection risks related to such processing. For processing activities that underwent a data processing assessment at an earlier point, or which have been registered with the Data State Inspectorate, a repeated assessment is not required unless the nature of processing or the applicable risks have significantly changed since the application of the GDPR.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that there are certain similarities among the tools that concern the corporate risks that are attributable to the data subject. Therewith, in case the credit institution performed the risk assessment of internal processes before 25 May 2018 (even in case it did not involve any specific marking out of data processing from the data subject's perspective) with the further registration of the data processing with the DSI, as well as if there were no significant changes in the registered data processing since its registration, the credit institution has satisfied the requirements regarding the assessment.

Scheme No. 1

Schematic representation of the necessity of a DPIA:



Methodology, content and format of a DPIA

The GDPR specifies that at least the following elements should be included in a DPIA:

1) description and assessment of envisaged processing activities;
2) description and assessment of envisaged purposes;
3) description and assessment of the legitimate interests of the credit institution or third party;
4) assessment of the necessity and proportionality of the processing operations in relation to the purposes;
5) analysis of activities to mitigate risks and demonstrate compliance with the GDPR.

The GDPR does not provide a specific methodology, content or format of a DPIA. Thus, the assessing party is free to choose the most suitable assessment methodology given the nature of their processing activities, and to expand the range of elements addressed in the DPIA.

In accordance with the Article 29 Working Party guidelines, the methodology of a DPIA should include at least the following criteria if one is to assume that the DPIA adequately considers all data processing aspects:

1) systematic description of the processing:
- **a)** specifying the nature, scope, context and purposes of the processing;
- **b)** noting the types of data, the recipients and the retention period;
- **c)** providing a functional description of processing and identifying processing assets (hardware, software, networks, people, documents, transmission/ communication channels);
- **d)** taking into account the compliance of processing activities with approved codes of conduct;

2) evaluation of the necessity and proportionality of the processing, including:
- **a)** compliance of the processing to specified, explicit and legitimate purposes;
- **b)** lawfulness of the processing;
- **c)** data adequacy and minimisation;
- **d)** data retention period;
- **e)** respect for data subjects' rights (e.g. information provided, access to data, rectification) and, if necessary, prior consultation with the supervisory authority;

3) management of risks to the rights and freedoms of data subjects:
- **a)** evaluating risk sources, nature, particularity, severity;
- **b)** evaluating potential impact on the rights and freedoms of data subjects (in the event of illegitimate access, undesired modification, disappearance of data) with regard to each potential risk, and specifying activities for remedying the risks;

4) involving interested parties (e.g. asking for opinion of the data protection officer, opinions of the data subject and their representatives).

DPIA plan

Because the Regulation does not specify a particular DPIA plan, the assessing party may select a DPIA plan that is appropriate given the nature of its processing activities. As mentioned hereinabove, the DPIA may be performed separately or integrated with another risk management process.
Assuming that a DPIA is carried out as a separate procedure, examples of the main steps to be taken within the DPIA framework are provided in the table below.[42]

[42] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Table No. 11

Example of a DPIA plan

Step	Action taken
Step No. 1	Establishment of the existence of data processing and need to assess
Step No. 2	Involvement of the interested parties (including consulting)
Step No. 3	Description of data and traffic
Step No. 4	Assessment of compliance (importance of purposes, data minimisation etc.)
Step No. 5	Identification of data protection risks
Step No. 6	Development of solutions
Step No. 7	Compilation and documentation of the DPIA results
Step No. 8	Integration of the DPIA results with the development and implementation of a business project
Step No. 9	Review and follow-up

However, considering the specifics of each credit institution, the organisation of the DPIA process may vary between different credit institutions as well as within a single credit institution (i.e. detailed assessment of processing activities that carry higher risk, assessment included in a different process etc.)

Persons involved in the DPIA

Overall, a credit institution is responsible for carrying out a DPIA; however, during a DPIA, the opinion of the data protection officer may be requested; independent industry experts can be involved as well; seeking the opinions of data subjects or their representatives (such as a trade union), and that of the processor (if one is to be involved in the relevant processing activities) is also recommended. It is advisable to also determine the opinions of structural units involved in data processing, such as the IT department, in order to seek advice regarding solutions, risk elimination or mitigation.

Combined or joint DPIA

A DPIA is not limited to a specific project. A combined DPIA may be carried out for multiple processing activities if the risks are similar and the nature, purpose, scope and context of each kind of processing is taken into account. One example could be plans to include the introduction of two new, mutually similar credit institution products (or a single product adapted to different customer segments) that require similar data processing. It is not necessary to assess each product separately – a combined DPIA for both products is permissible.

A DPIA is not limited to a specific controller; several controllers may conduct a joint assessment. For instance, if credit institutions have a joint project (implementing a new technology or solution), the credit institutions, possibly in cooperation with other industry representatives (such as the Finance Latvia Association), conduct a joint DPIA or, if a credit institution's group companies introduce a joint customer data processing system, the group of companies may conduct a joint DPIA for this data processing system.

Consultations with the supervisory authority

If the DPIA indicates that, despite the credit institution's reasonable planned measures to protect against and mitigate risk, a high risk to the rights of data subjects remains (e.g. data subjects may be subjected to substantial, irrecoverable consequences, or the identified risks are certain to occur), the credit institution should, prior to commencing data processing, consult this with the supervisory authority.

Disclosure of the DPIA

The DPIA does not require publication or other disclosure. However, the publishing of the DPIA, some part or summary thereof may facilitate trust for the credit institution and ensure complete adherence to the transparency and accountability principle.[43]

Where consultation with the supervisory authority is necessary, disclosure of the DPIA is required for the execution of this obligation. Likewise, disclosure is necessary to a greater or lesser extent, in order to ensure that other parties are involved in carrying out a DPIA or a joint DPIA. In any event, a credit institution is not obliged to disclose trade secrets in a DPIA.

Review of the DPIA and the processing

The GDPR states that the controller should evaluate the compliance of the processing with the DPIA at least in the event that the risk profile of the processing is changed. A repeated assessment of processing is also recommended to accommodate changes to the processing procedure or other external circumstances.[44]

Sample questions included in a DPIA

1) Is the necessity of processing a certain amount of data assessed? Can the purpose be achieved without processing the data, or processing to a lesser extent?
2) Are the data processing purpose and types of processed data (particularly Special Category of data) defined precisely? Is data processing consistent with the fulfilment of the purpose?
3) What is the legal basis for the data processing?
4) Will data processors be involved? Are appropriate contracts concluded with the processors entailing the right to control of the controller?
5) How frequently and in what way will the necessity and compliance of data processing to the processing purpose be evaluated?
6) How frequently and in what way will processed data be updated?
7) Is the range of (internal and third party) data recipients defined or is access by other parties restricted?
8) Are the period of retention and procedure of erasing data defined?
9) Are mechanisms specified for respecting the rights of the data subject (e.g. right to information, access)? Is a procedure defined for responding to the data subject's requests??
10) Are data recipients outside the EU clearly defined? Is the legal basis for such data transfer defined?
11) Are appropriate technical and organisational measures envisaged for ensuring data processing security?

For more information about the issues covered in this chapter – see Recitals 75, 76, 77, 84, 89, 90, 91, 92, 94 and 95 GDPR, and Articles 35 and 36 GDPR, as well as the Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of GDPR 2016/679" as of 4 April 2017.

6.4. Personal data breaches

What constitutes a personal data breach?

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted,

[43] Article 29 Working Party "Guidelines on Data Protection Impact Assessment and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" as of 4 April 2017.
[44] Ibid.

stored or otherwise processed. A security incident is different from a personal data breach (where damage is caused directly to natural persons' data, as opposed to e.g. legal entity data or a credit institution's property).

How can the impact on the data subject of a personal data breach be assessed?

Any physical, material or non-material damage to the data subject should be considered, including the data subject's loss of control over their data, or limitation of their rights, likelihood of discrimination, risk of identity theft or fraud, likelihood of financial losses, reversal of pseudonymised data, possible damage to reputation, likelihood of loss of confidentiality of data protected by a professional secrecy, or any other significant economic or social disadvantage arising for the relevant natural person.

Similarly, while evaluating the nature of a breach, one should consider the type of the breach (e.g. whether the data have been published or destroyed without justification), the nature of the data (e.g. Special Category of data, financial data, passwords) and amount, the likelihood of the data subject being identified, the significance of consequences for the data subject (from, for example, the publication of data that are already known to the public or those carefully kept from the public – in these two cases the consequences to data subject privacy will be different), data subject categories (e.g. children or people with health issues would face different consequences due to a breach), number of data subjects affected.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate indicated that the key criteria for the notification obligation are given in Article 33 GDPR. The DSI is of the opinion that there is no necessity to notify a personal data breach to the supervisory authority in case the violation is unlikely to result in a risk to the data subjects. However, the data controller shall internally register all identified data breaches and also justify why any risks are unlikely to be incurred and why such risks would not be high. Each case should be considered individually.

Also in situations when the breach has resulted in the disclosure of such personal data which allow identification of the natural person only by the data controller, e.g. card number or customer's number without any additional identifiers, the DSI may see the risks associated with the data subject as the card number might be known not only to the customer and the credit institution but also, e.g. to online stores. If, following the disclosure of the card number, the card is being blocked, it is rather unlikely that the breach will result in any risk to the customer. Whereas in the event the card is lost by the customer, in such a case it is not regarded as a data breach by the credit institution. The so-called "skimming" also does not constitute a breach, in case the credit institution has taken all the necessary technical and organisational security measures.

The DSI nevertheless recommends notifying of the breach to the DSI, in case the data controller has any concerns regarding the risk level caused by the personal data breach. In the opposite case – if the DSI learns about the breach from other persons, the DSI may impose a fine on the data controller for the failure to comply with the notification obligation, if it turns out that it is a case that had to be notified to the DSI.

Table No. 12

Does a personal data breach need to be reported?

Description of the breach	Report to the supervisory authority (without undue delay, not later than within 72 hours)	Reporting to the Data subject (without undue delay)
No risk group: a breach is unlikely to result in a risk to the rights and freedoms of natural persons.	×	×
Risk group: a breach that results in a risk that does not reach No risk group or High risk group.	✓	×
High risk group: a breach is likely to result in a high risk to the rights and freedoms of natural persons.	✓	✓

In accordance with the provisions of the GDPR[45], communication to the data subject is not required if any of the following applies:

- the credit institution has implemented appropriate technical and organisational protection measures, and those measures were applied to the data affected by the personal data breach – in particular such measures that render the personal data unintelligible to persons who are not authorised to access the data, e.g. encryption;

- the credit institution has taken subsequent measures to ensure that the aforementioned high risk (High risk group) to the rights and freedoms of data subjects is no longer likely to materialise;

- it would involve disproportionate effort. In such a case, there should instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

How should the supervisory authority be notified if not all the information to be communicated is known?

A notification to the supervisory authority should include the following information about a breach:

1) a description of the nature of the breach, including categories and approximate number of data subjects and categories of data affected
2) first name, surname and contact details of the data protection officer, or information about another contact point;
3) likely consequences of the breach
4) description of measures the credit institution has taken or intends to take to remedy the breach and/or mitigate potential adverse effects.

If, at the moment of notification, not all information has been compiled to ensure notification to the supervisory authority, the information currently known to the credit institution should be notified, supplementing and resending the notification to the supervisory authority as soon as possible.

Notification to the supervisory authority is required via its platform for reporting personal data breaches or by using its notification form. In cases where the platform for notifying personal data breaches is unavailable on the supervisory authority's website, controllers are entitled to use other means of notifying breaches (e.g. by submitting a document compliant with the law on the legal force of documents to the supervisory authority, and stating the aforementioned information).

[45] Article 34(3) GDPR.

Table No. 13

Example of personal data breaches and risk groupings

Description of the personal data breach	No risk group	Risk group	High risk group
Third parties have access to a customer's passwords and user names as a result of a cyber attack			✓
Unscheduled brief disruption within the internet banking system	✓		
Loss of a medium for storage (e.g. documents, CDs, USB carriers containing a contract drawn up with the customer) if the information is unencrypted and freely accessible			✓
Disclosure of information regarding a customer's transaction about which an article has been published by online news portals	✓		
Encryption key leak		✓	
Leak of encrypted data while the encryption key remains under the credit institution's control	✓		
Irreversible loss of data (e.g. physical destruction of data or destruction of the encryption key)			✓
Loss of a credit institution employee's computer with full drive encryption	✓		
Account statement sent to the other person's email address (not the customer's), if this other person can be considered a "trusted person"[46]			✓
Commercial messages sent to customers stating all addresses in a visible manner (e.g. using the "Cc" field instead of "Bcc")	✓		
Partial or complete loss of the customer database			✓
Unauthorised processing of customer data if happened within the credit institution and there is no risk to the customer		✓	

Each situation must be evaluated considering the nature and specifics of the relevant breach. This should be treated as an illustrative account helping to assess the severity of a personal data breach, prompting the assessment of cases where the data subject does not need to be communicated, as noted previously.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 7 March 2019, the Data State Inspectorate expressed an opinion that where the personal data breach involves sending of e-mail to the wrong recipient due to human error, the statement provided by the recipient on the deletion of the erroneously sent e-mail reduces the risks to the data subject. Nevertheless, in such case it is necessary to assess the risks and document the assessment as to why it is unlikely that the breach will result in a risk to data subjects. The DSI also recommends assessing the amount of the disclosed personal data, the nature and sensitivity thereof, including the possibility of the disclosed data being used, e.g. for fraud or identity theft. A material aspect for assessing the potential impact on the data subject is the confirmation of the wrong recipient that the data have been deleted and will not be used. In case no such statement is given, it does not automatically imply that the data subject is facing a high risk. It is recommended for the data controller to document its efforts to contact the wrong recipient and request to delete the erroneously received data and also to document the statement on the deletion of the erroneously sent data.

Moreover, the Data State Inspectorate is of the opinion that those incidents should be assessed on a case-by-case basis also when the data disclosed as a result of a personal data breach are subsequently found in public registers and databases, that can be accessed against payment or free of charge. The DSI considers that the amount of disclosed data should be assessed. i.e. whether only the data that are found in public registers have been disclosed.

[46] Article 29 Working Party "Guidelines on Personal data breach notification under Regulation 2016/679" as of 6 February 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

The DSI is of the opinion that a similar approach should be taken in cases when the data disclosed as a result of a personal data breach are encrypted by using modern encryption algorithms and the confidentiality of the encryption key is not compromised.

Should the identities of specific customers affected by a personal data breach be stated to the supervisory authority in a personal data breach notification?

The GDPR does not require notifying the supervisory authority about specific natural persons affected by a personal data breach but does require the specification of data subject categories and the approximate number of data subjects who have been likely affected by the personal data breach.

Should a personal data breach be notified if it has been remedied?

Remedying a personal data breach cannot obviate the need for a notification to the supervisory authority – breach recovery does not guarantee that data subjects will not be substantially impacted once their data have been affected by a personal data breach; reporting has the further purpose of allowing the supervisory authority to monitor the activities performed by the credit institution to prevent similar personal data breaches in the future.

When shall the supervisory authority be notified of a personal data breach ?

According to Article 33(1) GDPR, in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the supervisory authority of the personal data breach.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 March 2018, the Data State Inspectorate expressed an opinion that according to the Technology Subgroup of the Article 29 Working Party, the point of reference of counting the period of 72 hours after committing a personal data breach should be the moment when the controller discovers a personal data breach. Thus, the controller shall without undue delay submit to the DSI the initial notification and proceed with the assessment of all circumstances of the case (incident) and take measures to mitigate or eliminate the consequences of the breach.

The Data State Inspectorate is furthermore of the opinion that the controller should act on the basis of its own assumptions as regards the 72-hour time slot. However, in case of any doubts the incident should be reported as soon as possible. The DSI is of the opinion that an incident should be notified as soon as the controller has received answers to the questions contained in Article 33(3) GDPR. The DSI indicates that in case of delayed notification, the controller shall also specify the reasons for such a delay. The controller shall also record the assessment of the incident.

Who should notify a personal data breach?

During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 March 2018, the Data State Inspectorate noted that according to Article 33(1) GDPR, the obligation to notify a personal data breaches falls on the controller. In those cases when the controller is established in the European Union and has a branch in Latvia, the breach shall be notified to the lead supervisory authority in which jurisdiction is the investigation of the occurred personal data breach, as well as to other involved authorities. The personal data breach notification form[47] contains a section “Cross-border and other notifications” where the data controller indicates information on whether the notification is a cross-border notification that has been sent to the lead supervisory authority and that the data controller shall notify other involved authorities by giving a list of EU Member States to which the breach relates.

[47] LV-DPA, The personal data breach notification form: https://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/ (in Latvian).

The DSI additionally indicates that the controller shall notify a personal data breach committed by itself or its data processor. The GDPR does not oblige to notify breaches committed by other controllers.

For more information about the issues covered in this chapter – see Recitals 75, 76, 77, 85, 86, 87 and 88 GDPR, and Articles 33 and 34 GDPR, as well as the Article 29 Working Party "Guidelines on Personal data breach notification under Regulation 2016/679" as of 6 February 2018[48].

6.5. Guidelines for the use of technical resources and IT systems

The provisions of this subchapter have been developed based on the assumption that the credit institution and its systems are compliant with the Financial and Capital Markets Commission's normative regulations No. 112 "Normative regulations for the security of finance and capital market participants' information systems" as of 7 July 2015. These regulations set out the requirements for procedures for information system protection and technical solutions that protect against external threats.

In accordance with the GDPR, in order to ensure data processing security based on the degree of a risk (e.g. accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed), the credit institution should, in addition to the requirements specified in the aforementioned regulations, provide for the following measures:

1) data pseudonymisation and encryption
2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
3) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident
4) a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This aspect includes both the evaluation of all measures for network protection (firewalls, antivirus software, encryption of transmitted content, recording information on portable devices, device wiping in the event of loss or theft, etc., back-up solutions to ensure that data aren't permanently deleted, etc.), and physical security measures (e.g. physical protection of server rooms against break-in, server protection in the event of flooding, protection of portable storage media – USB flash memory, portable hard drives or CDs/DVDs, etc.). One should also evaluate the procedure of user identification, i.e. whether it is sufficiently secure – potentially evaluating whether two-factor authentication is required, such as a password and a physical means of identification (e.g. ID card).

The credit institution should provide documentation, and regular review and updating of each individual IT system involved in data processing.

Evaluation should include elements that may affect system reliability and the data contained therein:

1) ensuring that only authorised persons can access information resources (e.g. laptops, USB and tablet devices)
2) only appropriately authorised persons may perform any processing activities
3) storage of information on data actions performed (e.g. entry, correction, erasure, transmission to processor, transfer to third parties, time of transfer and recipient

[48] Article 29 Working Party "Guidelines on Personal data breach notification under Regulation 2016/679" as of 6 February 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

of information)
4) separation of distinct categories of data based on significance [for instance, "regular data" and Special Category of data (information on health condition)] with separation of access rights
5) ensuring that information carriers (DVD, CD, USB, hard drives) are destroyed entirely beyond recovery, and that the destruction is carried out by authorised persons only
6) assessment of requirements for password length and make-up (according to the latest security findings)
7) actions to be taken if a user's password becomes known to a third party (e.g. immediate blocking of user access)
8) data segmentation, isolating the active-use database from the passive one (restricting access to the latter to limit the risk of unlawfully obtained access to the active database, by keeping some part of the data stored securely in the passive database)
9) risk identification, assessment and seeking relevant solutions to prevent risks
10) data security out of office (such as encryption or remote data wiping)
11) software updates.

With regard to cloud data processing, one should evaluate whether a security audit is necessary, whether communications should be encrypted or what particular action must be taken to protect the data if cooperation is terminated (e.g. data deletion, recovery or deletion of back-up copies).

If the credit institution has lost the legal basis for subsequent use and processing of data as part of providing an everyday service, but maintains or establishes another legal basis (e.g. the customer has declined the credit institution's services but the data must be stored for accounting purposes), access to the data of such customers within information systems should be prohibited. Possible mechanisms would include data pseudonymisation and the creation of an archived copy of the relevant customer's entry, to which access would be allowed only in special cases, such as following requests by law enforcement or supervisory authorities.

Data encryption

The minimum measure recommended would include ensuring the encryption of:

1) all storage media that store or could potentially store personal data and which could become publicly available (e.g. portable USB memory devices)
2) data transmissions potentially containing personal data via public electronic communication networks.

Thereby it must be ensured that these data do not get unintentionally delivered to an unauthorised party. This kind of technical control would be advisable with regards to at least those credit institution employees who access (i.e. are authorised to receive) data from information systems, and to the relevant information systems and the data storage media used.

A uniform mechanism for transferring customer data to another market participant

The GDPR provides for a data subject's right to request the portability of data from one market participant to another. The recommended mechanism would involve the use of a uniform structured data format, such as XML (eXtensible Markup Language), allowing the export of a full copy of customer data in a format that can be read both by the data subject and by an information system, and ensuring the necessary data protection mechanisms for the secure portability of the data.

For more information about the issues covered in this chapter – see Recitals 74, 75, 76, 77, 78 and 83 GDPR, and Articles 24, 25 and 32 GDPR.

7. DATA PROCESSORS

7.1. Status of a data processor and division of responsibilities

What is a processor?

A processor is understood to be a business partner of a credit institution (a natural or legal person, public authority, or other separate body) that processes data on behalf of and in the interest of the credit institution based on a written contract, e.g. a credit institution's processor could be the partner that ensures the lease of servers used for storing the credit institution's data; a translation service provider, if the partner is provided with documents containing data for translation purposes; a provider of courier services if any personal data contained in the parcel are disclosed to him for further processing; a business partner (an agent) involved by credit institutions that ensure customer identification or communication with a customer.

A processor is considered to be a party in the "inner circle" of the controller; therefore, the processor does not require a separate legal basis for processing the credit institution's data besides the one used by the controller for the data processing; however, the processor shall undertake responsibility for the activities performed by the processor having been assigned the role by the credit institution.

In some cases, a credit institution may have processor status with regards to another controller, e.g. insurance intermediary by offering its customers life or non-life insurance services rendered by other companies.

In the given cases, the service provider is not considered a data processor. For example, a sworn notary should not be considered a data processor of a credit institution, as the notary does not carry out the processing of the data on behalf of the credit institution or in the context of data processing purposes set by the credit institution, but instead, is carrying out functions set out in the Notariate Law. In fact, the purposes of the data processing pursued by a notary are set in the Notariate Law, whereby the credit institution receives a legal service that is provided by the notary in his/her professional capacity. In the given case, both the credit institution and the notary act as a data controller and both of them have their own duties as regards personal data processing in the capacity of a data controller. A similar opinion has been expressed by the Information Commissioner's Office, ICO (United Kingdom) in its guidelines "Data controllers and data processors: what the difference is and what the governance implications are"[49].

Sworn attorneys and lawyers who process personal data for providing legal assistance also should not be treated as data processors. Equally, also sworn auditors or companies of sworn auditors should be treated as independent data controllers, if they process personal data for audit purposes on the basis of a written contract on auditing services.[50]

In case of doubt, wherever a credit institution wishes to clearly define the legal status of itself or a business partner with regards to the processing of certain data, a consultation with the supervisory authority is recommended.

[49] Information Commissioner's Office, "Data controllers and data processors: what the difference is and what the governance implications are", page 12: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.
[50] See: Article 29 Working Party "Opinion 01/2010 on the concepts of "controller" and "processor"" as of 16 February 2010, page 28: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Table No. 14

Who is liable for violations of the GDPR?

Liability	Controller	Processor
		Only if the processor has not complied with their duties under the GDPR or has acted contrary to the legitimate instructions of the controller.
Damage caused to the data subject by processing being carried out in violation of the GDPR	✓	✓
Imposing administrative fines	✓	✓

Processor's liability

The processor's liability with regards to lawful data processing may manifest in two ways if the processor fails to comply with the instructions given by the controller with regards to data processing, or if the processor fails to fulfil the obligations directly applicable to the processor under the GDPR. Regardless of the provisions of the contract between the processor and the controller, the processor also has the following direct liability under the GDPR when processing data upon the controller's assignment, such as::

1) not to involve subcontractors in the processing without the controller's written consent;
2) to cooperate with the supervisory authority if an audit takes place of the lawfulness of data processing by the controller
3) to ensure data security during processing
4) to maintain a register of processing activities concerning the data processed as a processor
5) to notify the controller about incidents (including personal data breaches) affecting data for which the processor is responsible
6) to involve a data protection officer, if it is necessary to involve one in accordance with the provisions of the GDPR.

Can a credit institution transfer liability to the processor under a contract?

No, the controller retains liability in the event of both potential administrative liability and in the event of potential claims by data subjects. The credit institution may file claims against the processor by way of recourse.

7.2. Choosing and contracting a data processor

The credit institution should develop internal regulations regarding how data processing that involves the processor is to be performed and monitored. The credit institution should ensure that the processor can maintain at least the same degree of data protection that the credit institution ensures for the relevant data categories.

The credit institution should provide the management of data processing by processors that defines the activities to be performed over the course of the entire data processing management life cycle handled by the processor. Data processing management applies to both external and internal service providers (within the group).

The processors' data processing management life cycle should include the following activities, which are to be documented by the contract owner or by another approved responsible person:

1. **due diligence** – initial due diligence of a potential processor referring to the competence and experience of the processor, their financial status, internal control environment, information system management framework, current certifications, potential conflicts of interest and other criteria approved by the credit institution as applicable to processor selection. An assessment of potential risks and their severity should be performed within the framework of due diligence;

2. **contract drafting** – while preparing a contract, the following aspects should be reviewed, while ensuring adequate risk monitoring:

    a) criteria for the assessment of processor activity and potential actions in the event of non-execution
    b) conditions for data processing
    c) obligations with regards to information security and carrying out of IT operations
    d) subcontractors involved in the processor's activity and their functions within the framework of providing the service
    e) data retention and storage locations
    f) whether contract termination will affect the continuity and quality of service provision
    g) the controller's and its auditors' right to access the information that ensures service provision, and upon receiving a notification in a timely manner, the processor must provide access to the processor's premises and other information allowing execution of the service
    h) the obligation to provide notification about events that might substantially affect the ability to provide service effectively in accordance with the provisions of the contract
    i) the obligation to provide documentation describing IT management, and the results of audit performed by third parties as necessary (e.g. external audit reports or IT security audits etc.)

3. **decision-making and contract signing** – it is recommended to engage the responsible structural units in the decision-making process for entering into a contract with the processor, for example, if a contract is concluded on providing a salary calculation service, then the human resources department should approve it. The credit institution should provide for the maintenance and updating of an internal register of processors, so as to monitor and keep records on processors involved.

4. **assessment and reporting** – it is recommended to conduct regular evaluations of the processor's service quality and effectiveness, assessing aspects such as incidents and the impact thereof on the credit institution – followed by decision-making regarding subsequent actions (carry on cooperation, amend the contract or discontinue the contract).

The European Banking Authority (EBA) has developed operational recommendations on outsourcing service management with regards to cloud service providers (EBA/REC/2017/03), which are advisable to follow for the purposes of ensuring a management process for outsourcing services.[51]

[51] See: European Banking Authority, Recommendations on outsourcing to cloud service providers: https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/e02bef01-3e00-4d81-b549-4981a8fb2f1e/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_EN.pdf.

What should be considered while selecting a processor?

Only those processors should be selected that provide adequate guarantees of implementing adequate technical and organisational measures to ensure compliance with obligations under the Regulation and protection of data subjects. A processor may justify the guarantees provided by adhering to and complying with an approved code of conduct or certification mechanism.

Necessity of a written contract

A written contract between the credit institution and a processor is required; otherwise, the processor will be considered a third party or a different controller, requiring a legal basis for the data transfer. Considering that the processor operates in the interest of and in a role assigned by the credit institution, a written contract will assist both parties in understanding their respective rights and obligations with regards to operations involving data transferred to the processor for processing purposes.

A written contract is also necessary if the processor transfers certain processing activities to a sub-processor, in which case the contract with the sub-processor must include provisions at least equivalent to those in the original contract with the processor.

During the meeting with the GDPR Working Group of the Finance Latvia Association on 21 March 2018, the Data State Inspectorate expressed an opinion that the GDPR does not oblige the data controller to enter into a separate data processing contract with the processor. The data processing that is carried out by the processor may also be governed by a cooperation contract. Moreover, it is not mandatory to include in the contract between the controller and the processor the terms “data processor” and “data controller” but rather provide a clear distinction between the roles and description of tasks. Each contract will be evaluated on a case-by-case basis, considering its essence and function.

Table No. 15

What requirements should be included in a processor’s contract?

Information included in a contract	Minimum requirements under the GDPR	Additional recommendations
1. Subject of the contract	☐	☐
2. Planned duration of a data processing (contract term)	☐	☐
3. Nature and purpose of data processing	☐	☐
4. Type of data transferred for processing	☐	☐
5. Categories of data subjects transferred for processing purposes	☐	☐
6. Rights and obligations of the credit institution:		☐
▪ to provide binding instructions in writing concerning technical and organisational measures applicable to the data processing		☐
▪ to monitor the ability of the processor to perform the contract and their obligations, and to ensure data security		☐
▪ to be able to unilaterally terminate the contract if the processor fails to fulfil its obligations under the contract or does not provide adequate measures for data protection		☐
7. Obligations of the processor:	☐	
▪ to only process data based on documented instructions from the credit institution (unless otherwise required by the EU or member state regulations binding upon the processor)	☐	

▪ to notify the credit institution about the fact of processing prior to commencing the processing if the processor is obliged to carry out processing of data transferred by the credit institution in accordance with the applicable legislation	☐	
▪ to ensure that persons involved in the processing have undertaken to observe confidentiality, unless such an obligation is specified in the applicable legislation	☐	
▪ to ensure that persons involved in the processing do not process data without being instructed to by the controller, and to ensure that they do not violate the instructions of the controller	☐	
▪ to implement appropriate technical and organisational measures for maintaining a level of security consistent with the assessed level of risk, such as: • data pseudonymisation and encryption • uninterrupted confidentiality, integrity, availability and robustness of processing systems and services • timely restoration of data availability and access following a physical or technical accident • regular testing, assessment and evaluation of technical and organisational measures to ensure the security of the data processing	☐	
▪ not to engage any other processor without specific prior written authorisation from the credit institution (or – if the credit institution allows the independent involvement of another processor in the contract – to immediately notify the credit institution once the involvement of another processor is known, thereby giving the credit institution a possibility to object to the involvement of such a processor)	☐	
▪ in the event of involving a processor (a subcontractor of the processor), to ensure that the other processor complies with the same obligations specified for the primary processor with regards to the processing of the credit institution's data	☐	
▪ taking into account the nature of the transferred data, to provide the credit institution with support for responses to a data subject's requests, and to ensure the fulfilment of data subjects' rights	☐	
▪ taking into account the nature of the transferred data and the available information, to provide the credit institution with support in ensuring the security of data processing	☐	
▪ to immediately notify the credit institution of an established personal data breach	☐	
▪ taking into account the nature of processing of the transferred data and the available information, to provide the credit institution with assistance in identifying and reporting personal data breaches to the supervisory authority and/or to data subjects	☐	
▪ taking into account the nature of processing of the transferred data and the available information, to assist the credit institution with the data protection impact assessments and/or prior consultations with the data protection authority	☐	
▪ following the provision of a service to delete or return all data (and deleting all copies) to the credit institution, in accordance with the interests of the credit institution, unless the applicable legislation of the EU or the member state requires storage of the data	☐	
▪ to provide the credit institution with all information necessary to verify the compliance of processing activities with the GDPR	☐	
▪ to provide auditors with access to the processor's premises and information, providing clarifications to auditors for the purpose of carrying out the audit of the processing of the transferred data	☐	
▪ to assign a data protection officer (if necessary in accordance with the GDPR)	☐	
▪ to cooperate with the supervisory authority if it exercises its investigative powers, including access to the processor's premises where the relevant data are processed	☐	
▪ to notify the credit institution about all requests by any data subject with regards to the processing of transferred data		☐
▪ to train the processor's staff in handling matters of data processing and with regards to the credit institution's instructions pertaining to processing of the transferred data.		☐

In accordance with Article 10.1 Credit Institutions Law, separate contracts with data processors must be coordinated with the Financial and Capital Markets Commission, and in such cases the regulations specified in the relevant regulation must be included.

For more information about the issues covered in this chapter –see Recitals 81, 82, 83 and 95 GDPR, and Articles 28, 29 and 32 GDPR, as well as EDPB "Guidelines 07/2020 on the concepts of controller and processor in the GDPR" as of 2 September 2020.[52]

[52] EDPB "Guidelines 07/2020 on the concepts of controller and processor in the GDPR" as of 2 September 2020: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

8. DATA PROTECTION OFFICER

8.1. Qualifications and guarantees of a data protection officer

Qualifications of a data protection officer

A data protection officer should be designated on the basis of their professional qualities and, in particular, their expert knowledge of data protection law and practices and the ability to fulfil the tasks specified in the GDPR. A person compliant with the provisions of the applicable legislation may be appointed as a data protection officer.

The most suitable candidates for the position of a data protection officer would be lawyers specialising in data protection and IT or certified information system auditors who possess specific knowledge regarding data protection law and practice.

A data protection officer must be able to conduct independent assessments of the credit institution's data processing despite having concluded an employment contract or service contract with the credit institution; they should also assist the credit institution or the credit institution's business partner in ensuring that the internal procedures and activities of the credit institution comply with the requirements of the GDPR.

Multiple data protection officers may be assigned; a data protection officer may also staff a professional team to ensure compliance with GDPR requirements in the operations of the credit institution, including communication with data subjects and cooperation with the supervisory authority on behalf of the data protection officer.

A data protection officer is considered to be an autonomous supervisor in the data protection area, since they play a substantial role within the data protection management system considering the requirements for assignment (the specific cases when assignment of a data protection officer is mandatory, their particular professional qualification requirements), their position (a responsible, independent expert in data-related matters) and tasks (monitoring compliance with the GDPR requirements, informing and advising, cooperating with supervisory authorities, etc.). Credit institutions should further ensure that a data protection officer and their team are able to fulfil their tasks effectively even if multiple credit institutions or units have the same data protection officer assigned to them.

Status of a data protection officer

Kredītiestādēm jāņem vērā, ka datu aizsardzības speciālistam nevar tikt dotas norādes Credit institutions should take into account that a data protection officer may not be given instructions regarding the exercise of their tasks, and the data protection officer is directly responsible to the highest management of the credit institution. Thus, the data protection officer should have such a status within the credit institution that their participation and opinion on data matters are adequately evaluated and perceived as an important and essential component of any process. Consequently, in order to ensure the authoritative status of a data protection officer, credit institutions must ensure that:

1. a data protection officer ensures the assessment of aspects of data protection at the credit institution, provides consultations to the credit institution and data subjects on matters of data protection, and cooperates with the supervisory authority in matters of data protection

2. a data protection officer is bound by confidentiality with regards to performance of their tasks

3. in the course of fulfilling their duties, a data protection officer duly takes into account the risk associated with the processing activities, taking into account the nature, scope, context, and purpose of processing

4. a data protection officer is involved in all questions related to data protection in an appropriate and timely manner

5. a data protection officer must receive support in fulfilling their tasks by being provided with the access to data and processing activities, as well as necessary resources for performing their tasks

6. a data protection officer does not receive any instructions regarding the performance of their tasks or the expected results thereof, including any instructions as to the interpretation or understanding of some matters of dispute

7. a data protection officer is allowed to carry out other duties at the credit institution, absent a conflict of interest

8. a data protection officer directly reports to the credit institution's highest management

9. the credit institution cannot delegate responsibility for the GDPR implementation to a data protection officer. Ensuring compliance with the GDPR is the credit institution's responsibility

10. a data protection officer has adequate working hours in which to fulfil their tasks

11. a data protection officer is granted an adequate supply of financial resources, infrastructure, and, if necessary, staff

12. a data protection officer is provided with regular training and opportunities to develop their qualifications

13. the functions of a data protection officer may not be isolated with regards to some part of the organisation's data protection activities only.

A data protection officer may be employed by the credit institution or involved as an outsourced service provider.

In summary, the credit institution's data protection officer is highly informed, duly supplied with the necessary resources, autonomous in their decision-making, and directly responsible for informing the credit institution's highest management regarding matters related to data protection, providing advice and suggestions or preparing a valid annual report for submission.

Taking into account that a data protection officer is directly responsible to the credit institution's highest management, it is acceptable for the management of the credit institution to conduct an assessment of a data protection officer's activity with the assistance of the credit institution's internal auditors. The internal audit may evaluate the activities of a data protection officer from a procedural standpoint, taking into account their independent status (i.e. a data protection officer may not be given instructions regarding the performance of their tasks), without evaluating the instructions given or opinions expressed by a data protection officer.

8.2. Prevention of conflict of interest

A data protection officer may also carry out other duties at the credit institution, provided that the data protection officer's activities do not present a conflict of interest.

One way to prevent a conflict of interest would be to envisage full-time employment for the individual carrying out the functions of a data protection officer (at least at the initial stage after commencing carrying out their duties as the data protection officer).

A conflict of interest may arise if a data protection officer performs duties that could directly affect the organisation's data protection activities which the data protection officer monitors.

A conflict of interest would most likely arise where the position of a data protection officer is held by a person who also holds a position in highest or middle management at the organisation (i.e. executive officer, operations officer, financial officer, IT department manager, HR department manager, legal department manager or marketing department manager), and specialists at other levels, provided that they are entitled to specify data processing purposes and means within the credit institution.

If a data protection officer carries out other functions within the credit institution, there should be a specific task plan for the activities of such a person while in the role of the data protection officer, ensuring that these activities do not overlap with other functions. An assessment of a data protection officer's performance must not be related to the assessment of their performance of other duties.

Even if a data protection officer is involved as an outsourced service provider, a conflict of interest may arise if the same party carries out other activities related to matters of data processing, such as representing the credit institution in court with regards to a personal data breach.

8.3. Designation of a data protection officer and contract termination

Is it mandatory for a financial institution to assign a data protection officer?

A data protection officer must be assigned if the core activities of the controller consist of processing operations which by their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale; or if the core activities of the controller consist of processing on a large scale of Special Categories of data, or data relating to criminal convictions and offences.

It must therefore be established that the provision of financial services, if they are rendered to natural persons, is consistent with these criteria, and credit institutions must assign data protection officers. If a credit institution does not provide financial services to individuals, the credit institution should evaluate the conformity of its activities with the aforementioned criteria in order to clarify whether a data protection officer must be assigned.

A common data protection officer for a group of companies

A group of credit institutions may appoint a shared data protection officer for several companies in the group, provided that the data protection officer is able to fulfil their tasks at all credit institutions involved in the group, and access to the data protection officer is available to all employees and data subjects (i.e. there is no language barrier and the data protection officer is available immediately when necessary). One data protection officer may be assigned to several group companies if the credit institutions have similar functions and are related geographically or organisationally.

Covering for a data protection officer in absence and termination of contract

The GDPR does not specify how and when a data protection officer may be covered for or fired but does state that they may not be terminated unfairly or sanctioned for the fulfilment of their direct tasks. Namely, a data protection officer may not be terminated, or sanctioned (e.g. by not providing benefits extended to other employees, or by impairing their career development), for providing an advice as regards data protection impact assessment. However, failure to provide such an advice in cases where it is necessary may be considered to represent a failure to duly fulfil obligations under the employment contract, for which a data protection officer may incur some liability by way of sanctions or the termination of legal relations.

Thus, a legitimate reason for firing a data protection officer may be related to, for example, theft or another gross violation of the regulations of the credit institution in its role as the employer, based on cases listed in the Labour Law which are not directly related to the fulfilment of the data protection officer's duties. However, in cases where a data protection officer provides data protection services under a concluded service contract, the terms and conditions of termination will be dependent on the provisions of such a contract. Thus, the credit institution may supervise a data protection officer to establish that their duties are fulfilled in accordance with the concluded employment contract or service contract.

In accordance with the requirements and duties specified for a data protection officer, as well as their obligations under the GDPR and employee rights under the Labour Law, the data protection officer may be covered for during their absence by another person who matches the requirements specified for a data protection officer.

If the functions of a data protection officer are carried out in accordance with a service contract concluded with a person or company that is not part of credit institution group companies, it is important to initially specify clear duties in the service contract, allocating specific functions to certain individuals, as well as specifying appropriate conduct in the event of the covering for the data protection officer.

In the event of the covering for the data protection officer, one should ensure that all the requirements specified for the position are fulfilled, including that there is no conflict of interests, that the person covering for the data protection officer is easily accessible via the specified contact details, and that there is no unfair sanctioning or termination. However, the credit institution should in each case individually evaluate the duration of the data protection officer's absence, the importance of data protection, and the potential impact on the decision-making of the credit institution.

8.4. Tasks of a data protection officer

A data protection officer's tasks and status:

1. informing and advising the credit institution and its employees involved in data processing about their respective obligations

2. supervising compliance with the GDPR and other normative acts (including internal regulations) on data protection, such as the division of duties, the notification and training of employees involved in data processing, and related audits

3. collecting information to identify processing processes, analysing and verifying the compliance of processing processes with the GDPR, and notifying, advising and guiding the credit institution on questions of data processing

4. upon request, providing advice regarding the data protection impact assessment and supervising its implementation

5. cooperating with the supervisory authority

6. acting as the credit institution's point of contact regarding matters of processing, including discussions prior to processing and other questions

7. providing consultations to data subjects that have contacted a data protection officer

Recommended:

1. providing a data protection officer with support from upper management to help them to fulfil of their tasks;

2. ensuring the participation of data protection officers in middle and upper management meetings;

3. involving a data protection officer in any decision-making process that affects matters of data processing, and providing them the opportunity to get acquainted with the relevant documents, express an opinion, and give advice;

4. consulting with a data protection officer in the event of a personal data breach;

5. clearly defining the tasks, status and functions of a data protection officer in the credit institution's internal regulations or in the job description, and including the relevant regulation in the contract concluded with the data protection officer;

6. if a data protection officer is unable to accomplish all of the specified tasks by themselves, or lacks the necessary knowledge or experience in certain fields (e.g. information systems auditing), the data protection officer can establish a separate team to ensure that these tasks are completed.

Decision-making

Decision-making regarding matters of data protection is carried out by the credit institution based on a data protection officer's opinion. Data protection officer does not take decisions.

For more information about the issues covered in this chapter –see Recital 97 GDPR; and Articles 37, 38 and 39 GDPR; as well as the Article 29 Working Party "Guidelines on Data Protection Officers ('DPOs')" as of 13 December 2016.

9. TRANSFERS OF DATA OUTSIDE THE EU

The EU, which is where the GDPR applies, provides a high level of protection to data subjects with regards to their rights, including lawful and proportionate data processing by credit institutions acting as controllers, and providing data subjects with the opportunity to control their data by exercising their rights to data erasure, rectification, portability, etc., and providing efficient protection of data subjects' rights within the framework of referral to supervisory authorities and contact with data processors regarding any damage caused.

Within the EU, the level of protection of rights ensured for data subjects should not be lowered if the data are transferred for a specific purpose (such as service provision or the observance of the legitimate interests of a credit institution) to controllers, processors or other recipients outside the EU. Transferring should be understood not only as the delivery of data to another controller or processor outside the EU; it also includes the placement of data (e.g. the location of a data server) within infrastructure sites owned by a credit institution in non-EU states. The preservation of EU-level legal remedies for data subjects may be ensured with the following set of tools.

The provisions of the GDPR update the existing principles for data protection to accommodate current requirements, including harmonisation and the development of unified conditions and requirements for the transfer of data outside the EU. At the same time, there is the option of establishing certification mechanisms, allowing clear indications that personal data processing activities performed by controllers or processors are compliant with the GDPR, and allowing controllers to develop unified codes of conduct as a way of facilitating appropriate and consistent implementation of the GDPR within specific industries.

9.1. Transfers on the basis of an adequacy decision

A credit institution may transfer data to a third country if the European Commission has decided that the territory of the relevant country, or specified sectors thereof, or the international organisation in question ensures an adequate level of data protection.

Information regarding decisions adopted by the European Commission is available on the website of the European Commission.[53]

9.2. Transfers on the basis of appropriate safeguards

If a credit institution needs to transfer data to a country outside the EU, with regards to which the European Commission has not adopted a decision regarding the adequacy of the level of data protection available there, a credit institution may send the data to the relevant third country or international organisation if the credit institution provides appropriate safeguards to the data subject, and effective means of legal protection are available to ensure that the rights of data subjects are respected.

How can appropriate safeguards be provided?

A credit institution may provide appropriate safeguards in one of the following ways:

1. by applying binding corporate rules to the data processing or to the data processor within the third country)
2. by applying standard data protection clauses adopted by the European Commission or the supervisory authority (and approved by the European Commission)
3. by applying a code of conduct approved in accordance with the GDPR to the

[53] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

third-country data recipient or processor
4. by applying certification mechanisms approved in accordance with the GDPR to the third country data recipient or processor
5. by applying a legally binding and enforceable instrument between public authorities or bodies
6. by receiving an authorisation from the supervisory authority, if a contract is being concluded with a third-country controller or processor without the standard clauses being approved as stated above.

9.3. Transfers based on derogations for specific situations

If a credit institution needs to transfer data to a country that is not an EU member state in the absence of an adequacy decision by the European Commission or appropriate safeguards, the credit institution may transfer data to the third country or international organisation only if one of the following conditions applies:

1. the data subject has explicitly consented to the transfer, based on sufficient information being provided prior to the transfer regarding the potential risks of such transfer
2. the transfer is necessary for the performance of a contract between the data subject and the credit institution or for the implementation of pre-contractual measures taken at the data subject's request (e.g. ensuring payment services or providing information to card organisations or correspondent banks for the purposes of performing contracts)
3. the transfer is necessary for the conclusion or performance of a contract, which is in the interest of the data subject, between the credit institution and another natural or legal person
4. the transfer is necessary for important reasons of public interest established by the EU or Latvian law (for example, for the exchange of information for the purposes of preventing money laundering and financing of terrorism as specified in the applicable legislation), and public interests should be interpreted narrowly in this case, applying this legal basis in cases of exception
5. the transfer is necessary for the establishment, exercise or defence of legal claims (e.g. litigation)
6. the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
7. the transfer is made from a public register (e.g. sending of information reflected in the land registry or registers maintained by the Register of Enterprises).

In accordance with Article 48 GDPR, a court judgment or decision of an administrative authority of a third country that requires a credit institution to transfer or disclose data may only be recognised or enforceable if it is based on an international agreement, such as a mutual legal assistance treaty between the requesting third country and the EU or the relevant member state. However, in this case, the credit institution should also take into account the data disclosure restrictions specified in Chapter V of the Credit Institutions Law.

If none of the aforementioned reasons for transfer of data apply, the credit institution may send the data as an exception, provided that the transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for compelling legitimate interests pursued by the credit institution which are not overridden by the interests or rights and freedoms of the data subject, and the credit institution has assessed all the circumstances surrounding the data transfer, and the credit institution has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data. In such cases, the credit institution informs the supervisory authority and the data subject of the transfer.

9.4. Assessing data transfers

To summarise the aforementioned, a credit institution should carry out a structured analysis of information and actions performed, in order to identify whether the transfer of data outside the EU complies with the provisions of the GDPR. An example of such an assessment is provided in the table below.

Table No. 16

Example assessment process for transferring data outside the EU

Analysis stage	Criterion	Examples
1.	Verify whether the European Commission has adopted a decision about a specific third country, its territories or specified sectors or international organisations, including them in a published list to indicate whether an adequate level of data protection is provided or not.	
2.	After verifying that the European Commission has not adopted a decision confirming the existence of an adequate level of data protection, the credit institution may transfer data to a third country or international organisation only if appropriate safeguards are provided and data subjects are provided with rights and effective legal remedies, namely: 1) the application of binding corporate rules, 2) the application of approved standard data protection clauses to the cooperation contract, 3) the application of an approved code of conduct, 4) the application of approved certification mechanisms, 5) the application of a legally binding instrument among public authorities.	In order to ensure fulfilment of corporate governance requirements or implementation of joint functions within the framework of a group of companies, exchange of data may be implemented based on approved binding corporate rules.
3.	The credit institution may provide necessary safeguards for data transfer by concluding a contract with the controller or the processor in a third country, without including the approved standard clauses mentioned in the previous stage. In such cases, an authorisation from a supervisory authority will be necessary..	
4.	Transferring or repeatedly transferring data to a third country or international organisation is possible if: 1) the data subject has explicitly consented based on information provided in advance, 2) a contract must be executed or action must be taken prior to conclusion of the contract upon the data subject's request, 3) important reasons of public interest apply, 4) the excercising or defence of legal claims is required, 5) the data subject is physically or legally incapable of consenting to the protection of either their own or other persons' vital interests , 6) the transfer is performed from a register to provide information to the public.	Exchange of information is necessary for the purposes of preventing money laundering and financing of terrorism. Transfer of information to a correspondent bank or card organisation to enable the execution of payment orders.
5.	If none of the necessary criteria mentioned in the aforementioned stages are met, the credit institution may transfer data to a third country or international organisation if: 1) the transfer is not repetitive, 2) the number of data subjects is limited, 3) the transfer is necessary for the legitimate interests of the credit institution, 4) the credit institution has evaluated all the circumstances and provided suitable data protection safeguards. The credit institution must inform the supervisory authority and data subjects about the transfer and the applicable legitimate interests. The credit institution must ensure that all stages are executed, safeguards are implemented, and the assessment is documented.	

9.5. Transfer of employee personal data

The work e-mail and phone number should be treated as credit institution's information that can be used by the credit institution at its own discretion, inter alia providing it to companies or credit institutions belonging to the same group. According to EU practice, an employee must use the work e-mail and phone number for professional needs and the employer retains the right to limit the use of the mentioned means of communication for private needs (inter alia prohibiting it entirely). It is recommended to regulate the use of work e-mail address and phone number with the credit institution's internal documents. The transfer of other employees' data to third countries must be regulated by the employment contract, considering the opinion of the Article 29 Working Party on the processing of employees' personal data at work.[54]

For more information about the issues covered in this chapter – see Recitals 101, 102, 103, 104, 105, 107, 108, 109, 110, 111, 112, 113, 114 and 115 GDPR, and Articles 44, 45, 46, 47, 48 and 49 GDPR.

[54] See: Article 29 Working Party "Opinion 02/2017 on data processing at work" as of 8 June 2017: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

10. COOPERATION WITH A SUPERVISORY AUTHORITY

Credit institutions undertake to cooperate with the supervisory authority in fulfilling its obligations. In accordance with the provisions of the GDPR, a credit institution must co-operate with a supervisory authority in at least the following cases:

1) a personal data breach – by notifying the supervisory authority about it and ensuring management of the consequences;
2) performance of a data protection impact assessment, provided that, despite technical and organisational measures, a high level of risk to the rights of the data subject applies;
3) notifying the supervisory authority about the assignment of a data protection officer.

If a data subject has complaints concerning the credit institution, they should, before contacting the supervisory authority, communicate with the relevant credit institution, and, if the matter cannot be resolved by involving the credit institution, the customer may then contact the supervisory authority.

Credit institutions support regular communication with the supervisory authority regarding current issues within the industry, including potential solutions to the issues in these Guidelines where possible.

Credit institutions engaged in cross-border data processing will mostly be supervised by the lead supervisory authority situated at the main establishment of their business. Thus, a credit institution should only cooperate with a single lead supervisory authority with regards to all data processing activities performed anywhere in the EU. Additional supervision may be performed by the local supervisory authorities within whose jurisdiction the data processing takes place, provided that such supervision is stipulated as an obligation in the local legislation or as an otherwise assigned public function.

To enable the local supervisory authority to receive control over data processing within its jurisdiction, one should contact the lead supervisory authority. The lead supervisory authority may allow or deny the local supervisory authority control over data processing that takes place within its jurisdiction. The main precondition for supervisory authority cooperation is that the activities of the authorities involved are in mutual agreement, avoiding any uncoordinated activities.

The European Data Protection Board may intervene in the operation of supervisory authorities if, for example, a local supervisory authority objects to the actions of the lead supervisory authority, and the supervisory authorities are unable to resolve the situation themselves.

It is possible that supervision will vary among different member states, because:

1) their data protection resources and attitude towards data protection may vary;
2) their practical implementation of applicable requirements may differ from the provisions of the Regulation;
3) a broad mismatch exists between the theoretical powers granted to member state authorities and the implementation of such powers in practice.

RESTRICTIONS ON USE OF THE GUIDELINES

The guidelines have been drafted in Latvian upon the assignment of the Finance Latvia Association, in accordance with the legislation and the Article 29 Working Party guidelines effective at the time, and considering the planned amendments to the legislation in the form of draft laws that have not yet been adopted or have not yet taken effect at the time of finalising these Guidelines.

The Guidelines are an explanatory, practical aid for the credit institution sector of Latvia during the preliminary period, allowing credit institutions to accurately implement the provisions of the GDPR, considering the opinions of the Article 29 Working Party and the guidelines it has issued or planned.

The Guidelines also include practical examples of the GDPR requirements, although the activities of each credit institution regarding the implementation of the GDPR provisions may vary based on the situation and circumstances applicable to a given credit institution – including types of products and services, number of customers, structure, IT system composition, internal regulations and current procedures.

These Guidelines should be considered in aggregate, since an analysis of individual parts in isolation may result in incorrect conclusions.

The conclusions and recommendations provided in these Guidelines are not binding upon supervisory authorities or other parties. The Guidelines are provided solely for reference for members of the Finance Latvia Association, and are not intended for other parties.