Privacy Protection Rules

Effective as of 30 June 2026

CBL ATKLĀTAIS PENSIJU FONDS

Content

Privacy Protection Rules

Effective as of 30 June 2026

1. About your privacy, why we care about it and protect it

Your privacy

Nowadays, technology is evolving very quickly, facilitating the rapid exchange of information and data, which can affect your privacy. Your privacy is important to us, so we do everything we can to protect it.

Financial security and secrecy of transactions

Our daily routine is to work with confidential and private information - your data, transactions, and other information. You entrust this information to us to receive quality services from us and special care for the security of your data and transactions.

Trust

Your trust is important to us, so we make sure your data is always safe.

Compliance with the law and best practices

We, AS "CBL Atklātais pensiju fonds", have developed these Privacy Protection Rules to provide you with general information about what data we process, why and how we protect it. You can also find information about data processing in applications, contracts, and other documents when you apply for our services.

If you want to receive information about the processing of your data, we will provide it in accordance with the procedure set out in these rules.

We provide this information in compliance with European Union and Latvian legislation, financial sector and supervisory authority guidelines, and best practices.

2. Let's get acquainted with the terms

bank – AS "Citadele banka".

Citadele Group companies – AS "Citadele banka" and all its foreign branches and subsidiaries.

consent – any freely and informed confirmation by which you consent to the processing of your data.

data – any information that concerns or could relate to you, such as your name, surname, personal identification number, address, phone number, email address, your habits.

Data State Inspectorate – an institution that supervises the application of the Regulation in the Republic of Latvia.

EU/EEA – European Union/European Economic Area.

Pension fund or we – AS "CBL Atklātais pensiju fonds".

processing – any actions we perform with your personal data, such as collecting, recording, storing, viewing, using, disclosing your personal data by sending, disseminating or otherwise making them available, coordination, deletion or destruction of your personal data, and more.

profiling – an automated method of processing your data to assess your economic, financial situation, personal preferences, interests, reliability, behaviour, etc.

regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

rules – these Privacy Protection Rules.

you – the person whose data we process.

3. Who processes your data

Your data is processed by AS "CBL Atklātais pensiju fonds", unified registration No. 40003397312, address: Republikas laukums 2A, Riga, Latvia, LV-1010.

If you have any questions regarding data processing, you can contact us by calling +371 67010147, or by writing to pfonds@cbl.lv or to our Data Protection Officer at gdpr@citadele.lv.

4. For what purposes, what data, on what basis we process, to whom we transfer it and how long we retain it

Before we collect your data, we always carefully assess why we need it. We process your data if there is a justification for doing so.

This may be in the following cases:

- **to enter and perform a contract:** We need data so that we can conclude a contract with you and provide you with a service.
- **to comply with legal requirements (statutory obligation):** We process data if we are obliged to do so to comply with the law, for example, to prevent money laundering or provide information to the relevant public authorities.
- **for public interests arising from the law:** We process data to help maintain security, order and fairness in society, for example in relation to the prevention of money laundering.
- **with your consent:** We only process your data if you have agreed to this, for example, to receive notifications and offers.
- **to protect important interests:** We process data to protect your and other persons` interests, such as life or health.
- **for archiving in the public interest:** We process data in accordance with the law to create and maintain archives for public interest.
- **to protect legitimate interests:** We process data when it is necessary to protect the interests of the pension fund, you or others.

What are legitimate interests? This justification allows pension fund to process data lawfully even if you have not given the pension fund special permission or the pension fund has not concluded a contract with you.

How does this work? The pension fund assesses whether the data processing is lawful, justified and necessary, and does not excessively interfere with your privacy. For example, pension fund may process your data for security purposes to prevent fraud.

How does this affect you? If the data is processed based on legitimate interests, you have the right to object to such data processing. The pension fund will carefully assess whether it is necessary to continue data processing.

4.1. Identity verification in person and in the electronic environment (authentication)

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Client identification in person	**Client or client representative** Name, surname, personal identification number, date of birth, number of identity document, date of issue, country, issuing authority, expiration date, photo, signature.	**Statutory obligation** • Regulation Article 6(1)(c) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines • Law on International and National Sanctions of the Republic of Latvia and other sanctions-related legal acts, guidelines **Public interest arising from the law** • Regulation Article 6(1)(e) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines	• Register of invalid documents • Cooperation partners who ensure identification when applying for services • Information systems maintainers	5 years from the date of termination of business relationship 10 years if the information has been requested by the supervisory authority or law enforcement authorities
Identity verification in the electronic environment (authentication) To use our services, we are obliged to verify your identity. Authentication is most often carried out using tools such as MobileSCAN/Digipass 780, Smart-ID, eID card or eParaksts Mobile, code card/code calculator. We do not process your biometric data (e.g. face or fingerprint data).	**Client/any natural person** Name, surname, personal identification number, device identifier, information specified in the application.	**Conclusion and performance of the contract** • Regulation Article 6(1)(b) **Statutory obligation** • Regulation Article 6(1)(c) • Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No	• Authentication service providers - SK ID Solutions AS, SJSC Latvian State Radio and Television Centre • Information systems maintainers	5 years from the date of termination of business relationship 18 months for storing online banking audit records.

This data is processed by companies that offer you authentication services.		1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 • Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council regarding regulatory technical standards on secure user authentication and common and secure open communication standards		

Pension fund must comply with Sections 26 and 27 of the Personal Data Processing Law, Article 44(3) of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, as well as Article 23 of the regulation, which sets limitations on individuals` rights to access information. These rules apply to the right to request information about data processing, its purposes, recipients, sources, as well as the right to access your data and request its correction, deletion, suspension, or restriction of processing.

4.2. Know your client (Client due diligence within the framework of anti-money laundering) and sanctions management

What is it?

As part of Know your client, pension fund checks who their client is to make sure they are not involved in illegal activities, such as money laundering.
“Money laundering” refers to the process of making money obtained through criminal activities — such as drug trafficking, human smuggling, and other unlawful activities, “dirty” money, is converted into “clean” money to make it look as though it was earned legally. Money laundering poses major threat to pension fund.

Countries have strict rules and laws requiring pension fund to identify, monitor, and report suspicious transactions to state authorities. Anti-money laundering measures implemented by pension fund helps to limit such activities.

As part of sanctions management, the pension fund monitors and complies with international and local sanctions. Pension fund carefully reviews client transactions to ensure that sanctioned individuals cannot receive services. Sanctions are applied to countries, organizations, or individuals that pose security threats, violate laws, or engage in illegal activities such as terrorism, money laundering, or human rights violations.

How does this affect you?

As part of Know your client, pension fund carefully checks the transactions (contributions) made and cooperate with state authorities. Please note that when providing services, pension fund may request documents and explanations required by law.

As part of sanctions management, when providing a service, pension fund may request additional documents and explanations regarding the transactions (contributions) made.

How does this affect us? If pension fund fails to comply with the rules, it may face significant financial penalties, suffer reputational damage, lose client trust, or even its license.

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Client due diligence before and during business relationships (We clarify the origin of funds, politically exposed persons beneficial owners and persons related to the client to comply with the legal requirements and identify suspicious transactions, as well as to ensure that international or national sanctions are not violated)	**Client (status of politically exposed person, beneficial owner (client or their family members or closely related persons))** Name, surname, personal identification number, birth date, place of birth, country, identity document number, issue date, issuing country and authority, expiration date, photo, nationality, address, phone number, email, social status/employer name, position, reputation, tax residence, source of income, amounts disbursed, information related to family members, kinship, politically exposed person (PEP) status, relationship with companies, shares, information related to client identification and research, signature.	**Statutory obligation** • Regulation Article 6(1) (c) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and related legislation and other related legal acts, guidelines • Law on International and National Sanctions of the Republic of Latvia and other sanctions-related legal acts, guidelines **Public interest arising from the law** • Regulation Article 6(1)(e) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and related legislation and other related legal acts, guidelines	• Public registers: Population register, Lursoft, Enterprise Register, State Revenue Service registers, Register of Invalid Documents • Information systems maintainers • Citadele Group Companies • supervisory and law enforcement authorities	5 years from the date of termination of business relationship 10 years if requested by the supervisory authority or law enforcement authorities

Freezing of funds and execution of the Financial Intelligence Unit's reporting and freezing of funds order	**Client** Name, surname, personal identification number, date of birth, information about the 3rd pension pillar agreement, payment details for freezing funds (payment date, amount, purpose of payment, payer/beneficiary account number), information related to the client identification and research.	**Statutory obligation** • Regulation Article 6(1)(c) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines • Law on International and National Sanctions of the Republic of Latvia and other sanctions-related legal acts, guidelines **Public interest arising from the law** • Regulation Article 6(1)(e) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines	• Financial Intelligence Unit • Information systems maintainers	5 years from the date of termination of business relationship 10 years if the information has been requested by Financial Intelligence Unit
Reporting suspicious transactions to the Financial Intelligence Unit (including, for violation or attempted violation of sanctions) and the State Revenue Service	**Client (status of politically exposed person, beneficial owner (client or family member or person closely related to him))** Name, surname, personal identification number, date of birth, place of birth, information related to client identification and research, signature, amount of contributions, accumulated 3rd pension pillar capital. Additionally, under sanctions management, citizenship, place of birth, country, information related to client identification and research.	**Statutory obligation** • Regulation Article 6(1)(c) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines • Law on International and National Sanctions of the Republic of Latvia and other sanctions-related legal acts, guidelines • 17.08.2021 Republic of Latvia Cabinet Regulation No. 550 Regulations Regarding the Procedures for the Submission	• Financial Intelligence Unit • State Revenue Service • Information systems maintainers	5 years after termination of business relationship 10 years if the information has been requested by supervisory authority, law enforcement authorities

		of Reports on Suspicious Transaction and the Threshold Declaration and Content Thereof **Public interest arising from the law** • Regulation Article 6(1)(e) • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing and other related legal acts, guidelines		

Pension fund must comply with Sections 26 and 27 of the Personal Data Processing Law, Article 44(3) of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, as well as Article 23 of the regulation, which sets limitations on individuals' rights to access information. These rules apply to the right to request information about data processing, its purposes, recipients, sources, as well as the right to access your data and request its correction, deletion, suspension, or restriction of processing.

4.3. **Pension funds' services**

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Provision of 3rd pension pillar services (individual membership agreement) (including identification, payment management, communication withing the service) As part of this service, you can make contributions to your 3rd pension pillar, build future savings, and increase your future pension.	**Client** Name, surname, personal identification number, date of birth, gender (for statistics), information about residency status, phone number, email, address, account number, signature. **Payer, if the payer is not a client** Name, surname, personal identification number, phone number, payers relation to the client. **Beneficiary/heir**	**Conclusion and performance of the contract** • Regulation Article 6(1)(b) **Statutory obligation** • Regulation Article 6(1)(c) - Law on private pension funds	• AS "Citadele banka" • information system maintainers	5 years from the date of termination of the business relationship

	Name, surname, personal identification number, date of birth, phone number, email, address, account number, signature.			
	For personal data used for identification, please refer to the section **Identity verification in person and in the electronic environment (authentication).**			
Provision of 3rd pension pillar services (collective participation agreement) (including identification, payment management) Your employer enters into an agreement with a pension fund and makes contributions on your behalf to the 3rd pension pillar of your pension. This means that a certain amount is regularly transferred to your pension account, and these savings are your property. The amount and procedure for contributions are determined by the collective participation agreement.	**Participant** Name, surname, personal identity number, date of birth, gender (for statistics), phone number, email, address.	**Conclusion and performance of the contract** • Regulation Article 6(1)(b) **Statutory obligation** • Regulation Article 6(1)(c) • Laf on private pension funds	• AS "Citadele banka" • information system maintainers	5 years from the date of termination of the business relationship
	For persona data used for identification, please refer to the section **Identity verification in person and in the electronic environment (authentication)**.			

4.4. **Organization of the pension funds' activities**

Purpose of data processing	Data types/sets (categories) we process	Justification for data processing	Data recipients	Data retention period
Physical security We ensure safety in the premises, territory, and other locations of the pension fund to protect	**Client, including a minor** Video image, name, surname, personal identification number, information indicated in the identity document,	**Legitimate interests** regarding the protection of the pension fund, your security and property protection, prevention and	• Cooperation partner providing physical security services	30 days

employees, clients, and property. Our purpose is to prevent and detect crime, control access, and provide evidence to protect the pension funds' interest.	information related to violations.	detection of possible crime, control of access to the pension funds' premises and collection of evidence in case of disputes or violations. • Regulation Article 6(1)(f)		
Attracting clients for the use of pension funds services (promotions, lotteries, raffles, contests)	The amount of data varies depending on the type of event. **Client** Name, surname, personal identification number, date of birth, phone number, email, data indicated in the identity document, tax residence, information related to the prizes won, account number, signature.	**Consent** to receive notifications and offers • Regulation Article 6 (1)(a) **Conclusion and performance of the contract** • Regulation Article 6 (1)(b)	• Cooperation partners providing the service	5 years
Maintenance and promotion of the pension funds' image (in-person and online events, social media and media)	The amount of data varies depending on the type of event. **Client, any person** Name, surname, phone number, email address, address, addresses of social accounts, audio recording, photograph, video recording, position, profession, type of occupation, length of service, employer, membership in professional associations, education, interests, use of 3rd pension pillar services and compliance with the client's needs. Any other personal data that you have disclosed at the event in written text/audio/photo/video, IP address.	**Conclusion and performance of the contract** • Regulation Article 6 (1)(b) **Legitimate interest** in creating and maintaining pension funds' image, attracting new clients, ensuring the trust and well-being of existing clients. • Regulation 6 (1)(f)	• Cooperation partners providing the service	10 years or, in some cases, longer to provide information on pension funds' history
Receipt and sending of documents (correspondence)	**Client/any natural person** Name, address, phone number, email, signature.	**Conclusion and performance of the contract** • Regulation Article 6 (1)(b)	• Postal service providers • Delivery and courier service providers	10 years

Storage and destruction of paper and electronic documents (Archiving)	**Client, any natural person, including a minor** Considering the amount of data and information specified in various documents, the following data is processed: Name, surname, personal identification number, date of birth, photograph, type of identity document, number, date of issue, issuing country, issuing authority, signature, phone number, address, email address, password for identification by phone, audio recording of the call, marital status, kinship, number of family members, employer, occupation, education level, nationality, validity and expiration date of residence permit , tax residence, taxpayer number, place of birth, country, nationality, information obtained during communication with the pension fund, authorization device, transaction history, information related to client identification and research, politically exposed person status, health data, account number, contributions made, information about financial knowledge.	**Statutory obligation** • Regulation Article 6 (1)(c) • Archives Law and state - defined document standards • Law on private pension funds • Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing • Law on International and National Sanctions and other sanctions - related legal acts • Law on Accounting • Civil Law and other regulatory acts **Archiving in the public interest** • Regulation Article 9 (2)(j)	• Cooperation partner providing the archive service, maintenance of information systems.	Various document retention periods (6 months, 5, 10 years)

4.5. **Receiving information, notifications and offers**

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Communication regarding your products and services, and their changes (via phone, email, the bank's online banking, mobile app, if you are bank client)	**Client** Name, surname, personal identification number, audio recording, video recording, phone number, email address, information about pension fund products, services you use.	**Conclusion and performance of the contract** • Regulation Article 6 (1)(b) **Consent** to receive notifications and offers	• Cooperation partners providing communication services	5 years from the date of communication

		• Regulation Article 6 (1)(a)		
Sending notifications and offers	Detailed information is provided in the Privacy disclaimer for the processing of personal data for receipt of notifications and offers.			

4.6. **Handling of requests, claims, applications and complaints**

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Handling applications, requests and complaints from individuals	**Client** Name, surname, personal identification number, date of birth, signature, audio recording, address, email, phone number, tax residence, account number, contributions made. Other types of data are determined depending on the scope of information requested in the request, claim, application, or complaint, as well as the information contained in the documents to be issued.	**Statutory obligation** • Regulation Article 6 (1)(c) • Law on private pension funds • Consumer rights protection law • Bank of Latvia Regulation No. 358 on the procedure for handling complaints received by financial market participants	• AS "Citadele banka", which provides processing of applications, requests, and complaints within the framework of 3rd pension pillar distribution services	5 years from the date the information is provided
	For personal data used for identification, please refer to the section **Identity verification in person and in the electronic environment (authentication).**			
Management of data subject requests	**Client** Name, surname, personal identification number, date of birth, address, email address, phone number, signature. Other types of data are determined depending on the scope of information requested in the request, , as well as the information contained in the documents to be issued.	**Statutory obligation** • Regulation Article 6 (1)(c) • Personal Data Processing Law	• AS “Citadele banka”	5 years from the date of providing the information

	For personal data used for identification, please refer to the section **Identity verification in person and in the electronic environment (authentication).**			
Examination of requests from the competent state authorities and their officials	**Client** Name, surname, personal identification number, date of birth, address, email address, phone number, signature, photograph, type of identity document, number, date of issue, issuing country, issuing authority, information contained in the documents to be issued, information related to family and children (name, surname, personal identification number, kinship), tax payment country, contributions made, debt obligations, taxpayer number, tax residence, place of birth, country, nationality, status of a politically exposed person, Other types of data are determined depending on the amount of information requested in the request, claim or application, as well as on the information contained in the documents to be issued.	**Statutory obligation** • Regulation Article 6 (1)(c) • Law on private pension funds • State Labour Inspection Law and other legal acts	• Bank of Latvia • Financial Intelligence Unit • Courts • Criminal Procedure Authorities • Police, Prosecutor's Office • Bailiffs • Notaries • Orphan's Courts • Data State Inspectorate • State Revenue Service • Information Technology Security Incident Response Institution • Ministry of Finance • Consumer Rights Protection Centre • Other officials specified my law	5 or 10 years from the date of providing the information, depending on the type of request.
Reporting (whistleblowing) on potential violations in the activities of the pension fund and protection of whistleblowers (You can report potential or identified violations, including possible fraud or criminal offences. We ensure proper protection of the whistleblower).	**Client/any natural person** Name, surname, email address, phone number, social media account addresses and content, video recording, information related to violations.	**Statutory obligation** • Regulation Article 6 (1)(c) • Whistleblowing Law	• AS “Citadele banka”	5 years from the date of reporting

4.7. **Provision of information and reports to supervisory authorities**

Purpose of data processing	Types/sets of data (categories) we process	Justification for data processing	Data recipients	Data retention period
Provision of information to the State Revenue Service regarding contributions made to the 3rd pension pillar agreement of termination of the agreement	**Client** Name, surname, personal identification number, contributions made, accumulated supplementary pension capital.	**Statutory obligation** • Regulation Article 6 (1)(c) • Law on personal income tax • Law on private pension funds • Regulation No. 899 "Procedure for the Application of the Norms of the Law "On Personal Income Tax""	• State Revenue Service	10 years from the date of providing the information
Provision of information to the State Revenue Service regarding amounts disbursed to the natural person	**Client** Name, surname, personal identification number, date of birth (non-residents), amount disbursed, withheld taxes and other payments. **Beneficiary/heir** Name, surname, persona identification number, amount disbursed.	**Statutory obligation** • Regulation Article 6 (1)(c) • Law on personal income tax • Law on private pension funds • Regulation No. 899 "Procedure for the Application of the Norms of the Law "On Personal Income Tax"" • Regulation No. 610 "Regulations on the Information to be Included in the Notification of Amounts Paid to a Natural Person"	• State Revenue Service	10 years from the date of providing the information

5. How we collect your data

We collect your data:

- When you give them to us:
- by using our products and services, which you can apply for at bank's client service centres, bank's mobile application, websites, bank's online banking, by filling out applications.
- when establishing a business relationship with the pension fund as required by law;
- if you have been designated as the beneficiary in the event of the death of the client;
- when contacting us via mail, email, mobile application, by phone, in person, by visiting bank's client service centres;

- when third parties give them to us:
- our cooperation partners who provide you with information about us;
- Citadele Group companies;
- maintainers of databases, registers, and media;
- state institutions and law enforcement authorities and their officials.

Your data is available only to our employees and those of our cooperation partners, who need it to perform their work duties and provide you with the necessary services. They process your data for certain purposes, in accordance with requirements of the law and the rules of pension fund.

6. Do we process data in an automated way and perform profiling

We process your data by performing profiling in certain cases. We do not process your data in an automated way.

Profiling

- **What is it?** Profiling is a data processing method where, using various personal data, we create your personal "profile," within which we assess data such as financial situation, transaction history, interests, demands, and more.

- **Why do we do this?** We perform profiling to:
- assess whether the relevant product or service is suitable for your demands and needs;
- assess risks;
- provide you with advice on 3rd pension pillar services;
- offer products and services tailored to your needs.

7. Do we transfer your data outside the EU/EEA

We process your data within the European Union and the European Economic Area. However, to provide certain services, data may be transferred to countries outside these territories, for example, if it is necessary for our cooperation partners to provide certain services. If we carry out such transfers, we will inform you. In such cases, we ensure that data is processed in accordance with the requirements of the regulation and is protected at the same level as required by the regulation.

If we transfer your data outside the EU or the EEA, we comply with at least one of the following conditions:

- we carry out the transfer to a country that has been recognized by the European Commission as safe for data protection;
- we transfer the data to a country or an international organization that guarantees security in accordance with specially adopted rules;
- the transfer of data is permitted by the Data State Inspectorate based on agreements between us and third parties (cooperation partners);
- you have given your explicit consent to the transfer of data;
- the transfer of data is necessary for the performance of a contract between you and pension fund or a contract with our cooperation partner in your interest;
- the data is transferred for the purpose of defending or exercising your rights, for example in legal proceedings.

For more information on data transfers outside the EU and EEA, visit the Data State Inspectorate's website: http://www.dvi.gov.lv. There you can also find the decision on countries that provide a level of data protection equivalent to Latvia's data protection level.

8. How long we retain your data

The length of time we keep your data depends on the purpose for which it is used. When determining retention periods, we consider the following criteria:

- **Performance of the contract:** We retain data for as long as necessary to ensure that the product or service is available to you.
- **Legal requirements:** We must keep data for a period specified by law, for example, 5 years from the moment the service contracts with you are terminated, as well as to comply with anti-money laundering regulations.
- **Protection of interests:** After the end of our cooperation, we retain data to protect your interests and ours, for example, for 5 years from the termination of service contracts with you.
- **Legitimate interests:** If the deletion of data could harm our, your, or third party interests, we will retain the data for as long as necessary.
- **Preservation of evidence:** We keep data to demonstrate that previous processing was lawful, for example, your consent to receive notifications and offers.

If the data is processed based on your consent, we retain it for as long as the consent is valid.

We follow industry guidelines when setting retention periods. If several valid periods apply such as those required by law and those necessary to protect our and your interests, we will keep the data for the longer period.

If none of these criteria apply, we will delete or anonymize your data.

9. What are your rights in relation to the data processing we carry out

When processing data, we ensure that you have the following rights by submitting a written request to us in free form:

9.1. **Withdraw consent for data processing**	If you have given consent, for example, to receive offers and notifications about our products, you can withdraw it at any time. You can withdraw your consent using: • online banking, if you are a bank client, • mobile application, if you are bank client; • email, • bank's client service centres by visiting in person. If you withdraw your consent, we will stop processing your data.
9.2. **Access your data**	You have the right to receive from us: • confirmation of whether we process your data; • detailed information about your data processing to ensure that the data is accurate and processed in accordance with the law. If you wish to access your data, please specify the exact time and the data you would like to receive. You have the right to know what data we hold about you, why we process it, how we obtained it, to whom we have disclosed it, and how long it will be retained. You may also request a copy of your data. To help us fulfil your request faster, please indicate the shortest possible time and describe precisely what data and information you would like to receive. Please note that we cannot be able to provide information if prohibited by law, for example, when providing data to law enforcement authorities (police, prosecutor's office, court, etc.).
9.3. **Correct data**	If you believe that the data we hold is inaccurate or incomplete, please let us know: • inform us about corrections needed; • we may ask you to provide documents confirming the necessary changes to the data, for example, if you have changed your surname.

9.4. **Delete data**	You can request the deletion of your data if you believe that: • it is no longer necessary; • it is not being used for the intended purposes. We will delete your data and inform our cooperation partners about the need to delete it, unless the data is required for the purposes for which we process it or the law requires us to retain it longer. Please note that it may not always be possible to fulfil a deletion request, for example, if the data is needed to provide you with a service, comply with legal requirements, or in legal proceedings.
9.5. **Restrict data processing**	You may request to restrict the processing of your data if: • you dispute the accuracy of the data (the restriction will apply until the accuracy is verified); • you believe the data processing is unlawful, but prefer to restrict rather than delete the data; • we no longer need your data, but you need it to defend your rights; • you object to data processing based on our legitimate interests. We will reassess whether, considering your objections, we need to continue processing data. If data processing is restricted, we will use the data only for specific purposes, such as defending our rights.
9.6. **Transfer data**	Data you have provided to us based on your consent or under a contract can be transferred. It is also possible to transfer data if we process it in an automated way. You can use this data yourself or, upon your request, we will transfer it to another service provider if there are no obstacles. When transferring data, please note that it may include third-party data, and its transfer must be assessed considering the rights and freedoms of third parties. To help us fulfil your request more quickly, please describe as precisely as possible what data and information you wish to transfer.
9.7. **Object to data processing**	You may object to the processing of your data if we process it based on legitimate interests. We will review your objections and assess the need to continue processing. We will need to continue data processing if it is necessary to comply with the law or to protect our rights. You will not be able to exercise the right to object to the data processing if you have given your consent to the data processing, if data processing is necessary for the performance of a contract, or if we are required to process the data to comply with the law.
9.8. **Refuse automated individual decision-making, including profiling**	We do not process your data in an automated way, including profiling.

10. How to submit a data processing request and how will we process your request

How can you submit a request?	What is the response time for processing your request?	What will be the fee for processing your request?	How will we provide a response to the request?
In writing, in free form: • in person, by visiting the bank's customer service centres, presenting an identity document – a passport or ID card, or a power of attorney if acting on behalf of someone else, • by email – assigning the request with a secure electronic signature, via online banking, if you are a bank client, using the mobile application, if you are a bank client, • via online banking, if you are bank client. Upon receiving your request, we will review it. If necessary, we will ask you to clarify the information and the data processing activities you would like to receive information about.	We will review your request: • not later than within 1 month from its receipt; • if the request is extensive or complex, we may need an additional 2 months. We will inform you about the period of extension and the reasons for it.	You can receive a response to your request: • free of charge; • if you submit a repeated request and we conclude that it is unfounded or excessive, we may apply a fee or refuse to fulfil the request. The fee will cover the costs of processing the information and the work of our employees. If payment is required, we will inform you in advance.	You can receive a response to your request: • in person, by visiting the bank's customer service centres, presenting an identity document—a passport or ID card, or a power of attorney if acting on behalf of someone else, • by email, receiving a password via SMS to access the document, • via online banking, if you are a bank client, We will take into account the way you provide us with a response.

11. What to do if you believe that we have infringed your rights by processing

We process your data in accordance with the regulation, European Union and Latvian laws, best practices in the financial sector, and guidelines and recommendations issued by supervisory authorities. If you believe we have violated your privacy rights, you can submit a complaint to us using the provided contact information. If the response does not meet your expectations, you can file a complaint with the Data State Inspectorate using the contacts provided:

AS "CBL Atklātais pensiju fonds"
Address: Republikas laukums 2A,
Riga, Latvia, LV-1010
Phone: +371 67010147
Email address: pfonds@cbl.lv
Data Protection Officer`s email: gdpr@citadele.lv

Data State Inspectorate
Address: Elijas iela 17, Riga, LV-1050
Phone: +371 67223131
Email address: pasts@dvi.gov.lv
Website: www.dvi.gov.lv

If the response from us or the Data State Inspectorate does not provide the desired solution, you have the right to apply to the court.

12. How do we keep your data safe

We protect your data against unlawful access, use, disclosure by taking the following measures:

We restrict access to the premises to unauthorised persons by ensuring:

- **Door locks (electronic doors):** We ensure all premises are locked when employees are not present.
- **Access control:** We use access cards (magnetic, chip cards), identity readers, code systems to control who can access the premises.
- **Selection of personnel:** We carefully select reliable employees.

We limit access to technological resources, ensuring protection of:

- **Technological devices:** Computer devices (desktop computers, laptops, tablets, servers), mobile devices (smartphones), communication devices (routers, modems), data storage devices (external hard drives, USB drives, SD cards), and other devices (printers, scanners, monitors);
- **Information systems, software, and applications**;
- **Communication networks and technologies** enabling data transmission and information exchange (internet, VPN, mobile networks, cloud technologies, etc.).

For the protection of technological resources, we provide:

- **Prevention of environmental threats:** We implement safety measures against fires, floods, large temperature changes and other conditions.
- **Prevention of technical risks:** We take care that there is a good power supply, uninterrupted power supplies in case of power failures and that other similar malfunctions do not occur.
- **Human threats:** We do not allow damage or theft.
- **Secure passwords:** We use secure and complex passwords for devices and accounts.
- **Screen locking:** When the device is not in use, we lock the screen.
- **User roles:** We limit access to data and systems, allowing only what is necessary for the relevant user.
- **Software and security updates:** We always install the latest versions to prevent vulnerabilities.
- **Encryption:** We encrypt data so that it cannot be accessed by third parties/unauthorized persons.
- **Secure connection:** We use HTTPS and VPN to ensure security when working online.
- **Antivirus:** We install and update antivirus programs on all devices.
- **Firewalls:** We use a firewall to protect the network from unwanted access.
- **Attack detection systems:** We install programs that monitor and warn about suspicious activity.

We carry out regular inspections and provide updates

- **Device checks:** We regularly check that all devices are in working order and in place.
- **System updates:** We install the latest software updates to address security risks.

We educate employees

- **Training:** We regularly inform employees about safety issues and how to act in suspicious situations.
- **Threat prevention:** We warn you about fraudulent emails and other potential security risks.

We monitor and analyse security

- **Log files (audit trails):** We record access and operations in systems so that they can be monitored and reviewed.
- **Regular tests:** We check the safety of systems to identify and eliminate potential risks.

We are ready for emergencies

- **Backups:** We regularly make backups of data and store them in safe places.
- **Emergency plan:** We prepare a plan for responding to threats to premises or technology.

Why is it important to us and to you?

Protecting technological resources helps protect data, prevent data leaks, theft, and guarantees that we can continue to work and avoid loss of money and reputation. Safety depends on each employee, so it is important to be careful and follow the rules.

Your data can only be accessed by pension funds' employees and cooperation partners who need it to perform their work duties. Before starting cooperation, we carefully evaluate the cooperation partners and inform them about the confidentiality and data protection. We and our cooperation partners ensure the protection and use of your data only for the intended purposes, in accordance with the requirements of the law.

13. How will we ensure up-to-date information about your data processing

To ensure that you are always informed about how your data is processed, we will regularly review and update these rules. Therefore, we invite you to review the latest version from time to time on banks and our website, in online banking and mobile application (if you are a bank`s client), or at bank's client service centres. If there are any significant changes, we will notify you one month before they take effect.