

Privacy notice for card users

Last modified 03.06.2023

About this notice and us



Who should read this notice? All payment card users. This document explains how we process your personal data if you have a payment card, whether physical or virtual, issued by Enfuce License Services Ltd. ("Enfuce" or "we").



Who are we and how to contact us? Enfuce is the issuer of your card and is the data controller for the personal data which you provide to us in relation to the card. Enfuce is an e-money and payment institution, authorised and regulated by the Finnish Financial Services Authority. Our registered office address is at Metsänneidonkuja 12, 02130 Espoo, Finland. If you have any questions about this privacy notice, how we process your personal data or you are looking to exercise your rights, please contact privacy@enfuce.com.



What is covered? This privacy notice covers how we use, look after, manage or otherwise process information that identifies you or could be combined with other information to identify you (referred to as personal data). Also, this notice covers your rights related to the processing of your personal data.

Enfuce is committed to protecting your privacy. We will process your personal data only in accordance with relevant data protection and privacy legislation and good data processing practices. Enfuce is the data controller of your personal data related to your payment card, which means that we define the purposes and means for processing of personal data and are responsible for the processing. Orka supports certain activities relating to your card and is a data processor of the personal data which you provide to us in relation to the card. Regarding your relationship directly with Orka, please see their privacy notice.










The sections below describe the following:

- What personal data we may process?
- Why and on which legal bases we process your personal data?
- Who can process your personal data?
- Where is your personal data located or transferred to?
- For how long we store your personal data?
- How we ensure the security of your personal data?
- What are your rights?

What personal data we may process?

Personal data means any information which can (or could be used to) identify a living person. We collect personal data from you when you apply for a payments card which is issued by us and when you use your card to make transactions. We also obtain information from third parties (such as identity verification or fraud prevention agencies) who may check your personal data against any information listed on population registers, sanction databases and/or other databases.

We have grouped together the types of personal data that we may process in the table below:

Types of personal data	
	Contact data – first and last name, email address, phone number, physical address
	Identification data – full name, address, phone number, email address, personal ID number, date of birth, nationality, national identification / social security number (SSN), signature, photo, other information on ID documents
	Payment transaction data – date, amount, currency, name of the merchant, creditor or supplier, transaction location, technical authorisation, clearing, settlement and routing data
	Payment card data – card number (PAN), card name, expiry date, CVV code, card PIN block, service code
	Card account information – information on account your card is linked to, such as account ID and account balance
	Technical data – such as data on system logs, IP address, cryptographic data
	Customer support data – information related to you included on customer support cases from your card program provider, such as account ID
	Information on political exposure and sanctions – data of persons constituting politically exposed persons ("PEP") and sanction lists, such as name, date of birth, place of birth, occupation or position, and the reason why the person is on the list in question
	Sensitive data – special categories of personal data that may be derived from transaction data

Sensitive / special categories of personal data

Processing of personal data about you that is very sensitive is only allowed in limited situations. Data protection legislation defines special categories of personal data as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership genetic data, biometric data for identification purposes, data concerning health or data concerning sex life or sexual orientation. Whereas we do not directly collect these types of data from you, sensitive personal data may be derived from payment transaction, for example when payment is done for a specific organisation, e.g. to a religious or political organisation.

Why and on which legal bases we process your personal data?

As a principle, we only collect your data to provide, manage and market our services or for purposes related to our business in general, such as for recruitment. Under data protection legislation, we can only process personal data for specific purposes. In addition, we always need to have a legal basis for processing personal data. The legal bases are defined in data protection legislation and include:

- To enter into and perform our **contract** with you: Your personal data is necessary to enter into a contract and carry out obligations in the contract with you, e.g. in order to provide you with a card issued by us.
- To comply with a **legal obligation** that we have: We may also process your personal data to comply with our legal or regulatory obligations, such as obligations related to identifying you as set out in anti-money laundering legislation.
- Your **consent** to us for processing of your personal data: We may process your personal data based on your consent where you have consented to processing for a specific purpose.
- To pursue our **legitimate interests**: We may have a legitimate interest to process your personal data where the processing is necessary to fulfil certain business requirements and the processing does not conflict with your rights, freedoms or reasonable expectations.

You can find out to which purposes and under which legal basis we process your personal data in the table below. For detailed listing of the types of personal data under each category, please see the section “What personal data we may process?” above. You can also find out if the data is collected directly from you or from other sources.

Purpose for processing	Categories of personal data	Legal basis	Collected from
Identification of you and verifying your identity as required in applicable legislation.	<ul style="list-style-type: none"> • Contact data • Identification data 	Legal obligation, performance of contract	<ul style="list-style-type: none"> • You, when you apply for a card • Other sources, such as Identity verification services and your card program provider
Setting up your account, including processing your application for a card and creating your account	<ul style="list-style-type: none"> • Contact data • Identification data • Payment card data • Card account information 	Performance of contract	<ul style="list-style-type: none"> • You, when you apply for a card • Other sources, such as Identity verification services and your card program provider
Maintaining and administering your account and the customer relationship	<ul style="list-style-type: none"> • Contact data • Identification data • Payment card data • Card account information • Payment transaction data 	Performance of contract	<ul style="list-style-type: none"> • You • Other sources, such as payment service providers, where applicable and your card program provider

Authentication for payment transactions	<ul style="list-style-type: none"> • Payment card data • Payment transaction data 	Performance of contract	<ul style="list-style-type: none"> • You, through technical means, when you make a transaction • Other sources, such as technical service providers and your card program provider
Processing your payment transactions, including authorization, clearing and settlement	<ul style="list-style-type: none"> • Payment transaction data • Sensitive data (see more information on section “Types of data”) 	Performance of contract	<ul style="list-style-type: none"> • You, through technical means, when you make a transaction • Other sources, such as payment service providers and your card program provider
Physical and virtual card management	<ul style="list-style-type: none"> • Contact data • Identification data • Payment card data 	Performance of contract	<ul style="list-style-type: none"> • You • Other sources, such as identity verification services and your card program provider
Monitoring your account for fraud	<ul style="list-style-type: none"> • Payment transaction data • Card account information • Payment card data 	Performance of contract	<ul style="list-style-type: none"> • You, through technical means when you make a transaction and your card program provider
Prevent, reveal and/or resolve issues related to money laundering and terrorism financing, including providing data to public authorities for investigation of such crimes in accordance with anti-money laundering and terrorism financing legislation.	<ul style="list-style-type: none"> • Contact data • Identification data • Information on political exposure and sanctions • Payment transaction data 	Legal obligation	<ul style="list-style-type: none"> • You • Other sources, such as our business partners, government-maintained lists or sources, financial service providers, identity verification and fraud prevention services, sanction list providers, public sources and payment service providers and your card program provider

Providing a secure environment for the transmission of our services	<ul style="list-style-type: none"> • Technical data 	Performance of contract	<ul style="list-style-type: none"> • You (through technical means)
Providing customer support related to your card, account or transactions	<ul style="list-style-type: none"> • Payment card data • Payment transaction data • Card account information 	Legitimate interest	<ul style="list-style-type: none"> • You (through technical means) • Other sources, such as your card program provider
Auditing and reporting	<ul style="list-style-type: none"> • Payment transaction data (in aggregated form) • Card account information (in aggregated form) • Contact and identification data • Technical data (in aggregated form) 	Legitimate interest	<ul style="list-style-type: none"> • You (through technical means) • Other sources, such as payment service provider, where applicable and your card program provider
Ensuring and developing security of our systems with technical means, such as with data encryption, access controls, log management and auditing	<ul style="list-style-type: none"> • Technical data 	Legitimate interest	<ul style="list-style-type: none"> • You (through technical means)
Promote, analyse, modify and improve our systems, and tools, and develop new services	<ul style="list-style-type: none"> • Technical data 	Legitimate interest	<ul style="list-style-type: none"> • You (through technical means)
Conduct aggregate analysis and develop business intelligence that enable us to operate, protect, make informed decisions, and report on the performance of, our business;	<ul style="list-style-type: none"> • Payment transaction data (in aggregated form) • Card account information (in aggregated form) • Technical data (in aggregated form) 	Legitimate interest	<ul style="list-style-type: none"> • You (through technical means) • Other sources, such as payment service providers (where applicable)

	<ul style="list-style-type: none">• Customer support data (in aggregated form)		
--	--	--	--

Who can process your personal data?

Your personal data is processed only by personnel who are authorized to do so based on their role. Enfuce does not sell your personal data.

Your personal data can only be transferred or disclosed to the following categories of third parties, in the following situations:

- **Our group companies:** Enfuce group companies are involved in processing of your personal data, including processing of your payment card transactions.
- **Our service providers:** We use service providers in order to manage and operate our business. Service providers are needed for a variety of purposes, such as operation of our IT systems. These service providers can only process your personal data based on our instructions and use it only for purposes defined by us. Such processing is always regulated by data processing agreements in order to ensure that all our service providers keep your personal data safe and process it only in accordance with applicable legislation.
- **Your card program provider:** your card program provider supports certain activities relating to your card, such as verifying your identity.
- **Identity verification and sanction list agencies** to undertake required verification, regulatory and fraud prevention checks;
- **Regulatory and law enforcement authorities** where the law requires us to do so.
- **Anyone to whom we lawfully transfer or may transfer our rights and duties under the agreement;**
- **Any third party as a result of any restructure, sale or acquisition of Enfuce or any associated entity,** provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us.

Where is your personal data located or transferred to?

We may transfer your personal data within Enfuce group companies in countries where Enfuce has operations.

We store your personal data in servers located in the European Economic Area (EEA), but we may use service providers that are based elsewhere in limited occasions. In cases where your personal data may be transferred outside of the European Union (EU), the European Economic Area (EEA), the United Kingdom (UK) or Switzerland, we ensure the lawfulness of the transfer using a valid legal mechanism. These mechanisms include adequacy decisions adopted by the European Commission concerning a specific country and European Commission's Standard Contractual Clauses for international transfers of personal data. In addition, we use additional security safeguards such as encryption to ensure the security of the personal data transferred.

For how long we store your personal data?

The storage period for your personal data depends on the purpose it is processed for. We only retain your personal data for as long as is required for the purpose. Legislation applicable to us, such as anti-money laundering legislation, sets out mandatory retention periods that define for how long we store your personal data. Where there is no legal obligation to store certain personal data, the retention times are defined based on our legitimate business needs. The following table illustrates retention periods and criteria for defining retention periods for key types of personal data.

Types of personal data	Retention period and/or criteria for defining it
Information used for identification and identity verification	<ul style="list-style-type: none"> Six years after the end of the customer relationship, based on anti-money laundering legislation
Payment transaction-related data	<ul style="list-style-type: none"> Six years after the end of the customer relationship or after an occasional transaction, based on anti-money laundering legislation

How we ensure the security of your personal data?







Enfuce is committed to maintaining the security of your personal data with state-of-the-art technical and organisational security measures. We secure the confidentiality, integrity and availability of your personal data, and protect it against loss, misuse, unauthorized access, disclosure, alteration and destruction. These measures include, inter alia:

- advanced encryption of data both in transit and at rest;
- pseudonymisation of personal data;
- role-based access controls and user authentication;
- technical IT and network security measures;
- comprehensive information security policies and staff training in accordance with them;
- incident and breach management processes;
- business continuity and disaster recovery processes;
- regular testing and review of our security measures;
- agreements covering data protection and security measures with our partners.

What are your rights?

You have specific legal rights in relation to your personal data. If you would like to exercise any of your legal rights, please contact: privacy@enfuce.com.

Your data protection rights are as follows:

	Right of access: You have the right to know whether we process your personal data and to know what personal data about you we process. You may request for a copy of such data.
	Right to rectification: You have the right to correct and update your personal data or ask us to update it if it is inaccurate or incomplete. We encourage you to keep all your personal information up to date.
	Right to erasure ("Right to be forgotten"): You have the right to request us to delete your personal data. We will delete your personal data unless we have a legal obligation or other overriding reason to retain your data. In such case, we will let you know and explain our decision.
	Right to restriction of processing: You can, under certain limited circumstances, ask us to restrict how we use your personal data and temporarily limit the way we use it (e.g. whilst we check that the personal data we hold for you is correct).
	Right to objection: You can object to us processing your personal data if you want us to stop using it, provided that our legal basis for processing that personal data is legitimate interest or in relation to marketing communications.
	Right to data portability: You can ask us to send you or another organisation an electronic copy of your personal data, provided that the processing is based on performance of a contract with you or on your consent.



Complaints: If you are unhappy with the way we collect and use your personal data, we hope we can resolve it. Please contact privacy@enfuze.com in the first instance. However, if you consider that our processing infringes your rights as a data subject, you always have the right to complain to a data protection supervisory authority, in the country where you work, normally live or where any alleged infringement of data protection laws has occurred. The supervisory authority in Finland in the Office of the Data Protection Ombusman, www.tietosuoja.fi.

The supervisory authority Denmark is: The Danish Protection Agency, +45 33 19 32 00, Datatilsynet, Carl Jacobsens Vej 35, DK-2500 Valby

Can this information be changed?

Our services and applicable laws are continuously developing. There will be updates to this privacy notice whenever changes or developments require so. The up-to-date version of our privacy notice can always be found on our website at <https://enfuze.com/privacy-notice/>. The date of this notice can be found at the top of the page. We recommend that you revisit the page from time to time to review any possible changes. If any substantial changes in the way we process your personal data occur, we will post a notice of such change on the website.