

Visa Open Banking Privacy Notice for End-Users

Effective date: 04/11/25

Visa values your trust and respects your privacy. This Open Banking Privacy Notice for End-Users ("**Privacy Notice**") explains how Visa and/or its Affiliates¹ including Tink A.B. and Tink Financial Services Limited ("**Visa**", "**we**," and/or "**us**") collect, use, and share your Personal Information when you use our Open Banking Services (as defined below), and related services that link to this Privacy Notice. The relevant controller for this Privacy Notice is the entity with whom you have agreed terms of service for the Open Banking Services.

To learn more about how Visa collects, uses and shares Personal Information please visit Visa's website to access the Visa Global Privacy Notice and [Visa Privacy Centre](#).

¹ Affiliates are companies related by common ownership or control, including Tink A.B. and Tink Financial Services Limited. [↩](#)

What is covered by this Privacy Notice?

1. [About Our Open Banking Services](#)
2. [Scope of this Privacy Notice](#)
3. [Categories of Personal Information](#)
4. [Sources of Personal Information](#)
5. [Retention of Personal Information](#)
6. [Why We Collect Personal Information and How We Use It](#)
7. [Categories of Third Parties and Our Disclosure of Personal Information](#)
8. [Profiling and Automated Decision-Making](#)
9. [Your Privacy Rights](#)
10. [International Transfers](#)
11. [Information Security](#)
12. [Changes to this Privacy Notice](#)
13. [How to Contact Us](#)

About Our Open Banking Services

The open banking platform enables our business customers ("**Partners**") to build services that leverage financial information of individuals ("**End Users**" or "**you**").

We provide account information services, payment initiation services, and other related open banking solutions ("**Open Banking Services**") to End Users and Partners, which allow End Users to share their financial information with Partners or to make payments.

When you request services from a Partner, the Partner will redirect you to the open banking platform, where we can collect your financial information or initiate a payment on your behalf. Once this process is concluded, you are redirected back to the Partner.

Scope of this Privacy Notice

We fulfil many roles when providing our Open Banking Services.

When we provide Open Banking Services directly to End Users, End Users will sign up to our End-User Terms of Service. In this scenario, this Privacy Notice applies to the collection, use and sharing of End Users' Personal Information that we process in connection with the provision of the Open Banking Services.

We may appoint Partners as agents as described in the applicable terms of service. Please refer to the relevant Partner's privacy notice, should you have questions about their practices. In some circumstances, we act as a joint controller together with the Partner. This means that we both have certain responsibilities under data privacy laws. Where this is the case, we have agreed with the Partner that the Partner is responsible for providing you with

information about how your Personal Information is processed and for enabling you to exercise your rights under applicable data privacy laws.

When we act on behalf of Partners, we only collect, use, and share Personal Information as authorised by contracts with Partners. In this scenario, the privacy notice provided by the Partner with which you have a relationship will apply and this one does not apply. This Privacy Notice does not cover what others, such as Partners, websites or other applications, do with your Personal Information. This Privacy Notice also does not cover Personal Information we collect through our website, or when you interact with our websites. Please read the privacy notices published on our websites or otherwise provided to you when you interact directly with us.

In this Privacy Notice, "**Personal Information**" refers to information that (alone or when used in combination with other information) is capable of being associated with or could reasonably be associated with an individual. Personal Information, sometimes referred to as "personal data", may also have specific meanings under different privacy laws. The Personal Information we collect varies depending on our relationship and interactions with you.

Categories of Personal Information

Depending on our relationship and interactions with you, the categories of Personal Information we collect may include:

- **Contact Information** – this includes your name, title, date of birth, username, mailing address, email address, telephone number and mobile number.
- **Identity Information** – this includes Government-issued identification documentation, such as a national insurance number, driving licence, passport, and other Government-issued identifiers.
- **Transaction Information** – this includes:
 - information about your transactions, including purchases, description, currency, date, time, location, amount of the transaction, source, destination, remittance information and information about the merchant. This may also include item-level data in some instances, and billing and shipping information; and
 - information about initiated payments, including payment description, amount, currency, date, source, destination and registered beneficiaries.
- **Account Information** – this includes bank account number, bank account title and type (e.g. loans, mortgages, savings, investments, pensions, credit card, checking accounts), account balance, credit limit, overdraft limit, account turnovers, standing orders, scheduled transfers, bank name and branch location.
- **End User Authentication Data** – this includes the information you use to log in to your bank, such as your bank username, password, PIN code, national insurance number, email address, phone number, date of birth and the unique authentication token used to identify you as the owner of your account.
- **Inferred and Derived Information** – we infer and derive data elements by analysing our relationship and transactional information. For example, we may generate propensities, attributes, and/or scores for marketing (where permitted), security or fraud purposes.
- **Online and Technical Information** – this includes information about how you use our Open Banking Services and your interactions with websites or applications that you use to access the Open Banking Services, including IP address, user ID, bank name, market/region, location, device identifiers, settings, characteristics, activity log records, and other information collected using cookies and similar technologies.
- **Support Data** – customer support dialogue data.
- **Compliance Data** – this includes records we maintain to demonstrate compliance with applicable laws such as the anti-money laundering checks we conduct, records related to consumer preferences, and records related to data subject rights requests.

Sources of Personal Information

We may collect Personal Information about you from various sources, depending on our relationship and interaction with you.

We may collect Personal Information:

- from you – (we also receive Personal Information of third parties from you, when we process the data of individuals appearing in your transactions e.g. your payers and/or payees and their Personal Information does not come to us directly but through their dealings with you);

- from Partners – depending on the Open Banking Service you use, we may collect your Personal Information from Partners;
- from your bank – the Open Banking Services may require us to collect Personal Information from your bank. We will collect this type of information with your consent where we are required by applicable law;
- from your computer or devices – we may collect Personal Information when you use our Open Banking Services on your device;
- from our Affiliates; and
- from other sources – when you use our Open Banking Services, we may receive identifiers and commercial information about you from other third parties including our service providers, identity verification services and publicly available sources.

Retention of Personal Information

We retain your Personal Information for as long as the information is needed for the purposes listed below and for any additional period that may be required or permitted by law. The length of time your Personal Information is retained depends on the purpose(s) for which it was collected, how it is used, and the requirements to comply with applicable laws. When it is no longer needed, the Personal Information is securely deleted or (where permitted by law) anonymised. You may request that we delete your Personal Information by visiting our website and accessing our [Privacy Rights Portal](#). If we do not have a legal basis for retaining your Personal Information, we will delete it as required by applicable law.

Why We Collect Personal Information and How We Use It

Why We Collect Personal Information and How We Use It (where you are required to provide Personal Information so that we can deliver our Open Banking Services, we have marked this with a *)

Why We Collect Personal Information and How We Use Its		
Purpose of Processing	Categories of Personal Information	Lawful Basis (where required by applicable law)
Delivery of our Open Banking Services including aggregation and transfer of account information and administration of our account information and payment initiation services.	• Identity Information* • Contact Information* • Transaction Information* • End User Authentication Data* • Inferred and Derived Information* • Online and Technical Information* • Account Information* • Support Data*	• Performance of a contract.
Provide customer support to you or Partners in connection with our Open Banking Services.	• Identity Information • Contact Information • Support Data	Our legitimate Interests to maintain appropriate standards of service.
To comply with applicable laws regarding our Open Banking Services (including security, anti-money laundering requirements, know your customer requirements, requirements on incident management, fraud prevention, consent management and transaction log keeping).	• Identity Information* • Inferred and Derived Information* • Contact Information* • Account Information* • Transaction Information* • Financial Information* • Online and Technical Information*	Compliance with our legal obligations.

Purpose of Processing	Categories of Personal Information	Lawful Basis (where required by applicable law)
Where and to the extent permitted by applicable law, to ensure the effective running of our business including processing as necessary for the purposes of (i) enforcement of contracts; (ii) contract management; (iii) account management; (iv) quality control; (v) fraud prevention; (vi) corporate governance; (vii) reporting; and (viii) disaster recovery and business continuity.	Where compliance with these obligations involves the processing of criminal offence data (e.g. when we are performing sanctions checks), we shall only conduct such processing where permitted by local law. • Identity Data • Contact Information • Account Information • Transaction Information • Inferred and Derived Information • Online and Technical Information • Geolocation Information • Compliance Data	Our legitimate interests to ensure the effective running of our business.
Where and to the extent permitted by applicable law: • generate de-personalised, de-identified, anonymised, derivatives, compilations, combinations or aggregated datasets, which are used for product development and enhancement, troubleshooting and compliance reports; • understand how you and others use our Open Banking Services, for analytics and modelling and to create business intelligence and insights and to understand economic trends; • develop and offer products and features based on artificial intelligence-based systems that can identify and categorise financial risk patterns; and • personalisation and preference management and providing product updates.	• Transaction Information • Account Information • Inferred and Derived Information • Online and Technical Information	Our legitimate interests to perform analysis and take steps to aid the progression of our business.
To manage and/or administer the sale of our business or any assets (including mergers, acquisitions and divestitures).	• Identity Information • Transaction Information • End User Authentication Data • Inferred and Derived Information • Online and Technical Information • Support Data • Compliance Data • Account Information	Our legitimate interests to manage our business.

Categories of Third Parties and Our Disclosure of Personal Information

Your Personal Information is primarily shared with the Partner whose Partner Service(s) you utilise and whom you have instructed us to make the data accessible to.

Your data may also be shared with:

- our Affiliates;
- your bank when you request that we provide our Open Banking Services. The login details you have shared with us are only disclosed to your bank and only when the respective services are performed.
- Partners, banks (or their authorised processors), data aggregators, payment processors, and other third parties that are subject to appropriate confidentiality and use restrictions, for the purposes of providing Open Banking Services to you, managing fraud and risk, providing and developing our Open Banking Services, and supporting the purposes outlined in the table above;
- regulators and other law enforcement authorities (such as the police or HMRC) to comply with our legal obligations or investigations;
- courts, other parties to a litigation and our professional advisors; and
- our service providers, such as software and data storage providers who process your Personal Information on our behalf and strictly in accordance with our instructions.

We may disclose Personal Information with other third parties with your consent, or as permitted by law, such as when we sell or transfer business assets, enforce our contracts, protect our property or the rights, property or safety of others, or as needed for audits, compliance and corporate governance.

Profiling and Automated Decision-Making

"Profiling" is when Personal Information is automatically processed for the purpose of evaluating certain personal aspects relating to the individual, such as an individual's economic situation or personal preferences.

"Automated decision-making" is when automated means without human intervention are used for making a decision in relation to an individual, such as denying an individual to use a service.

We may use automated decision-making, including profiling, when processing your Personal Information in connection with providing Open Banking Services for the purpose of fraud prevention. This processing is based on our legitimate interest and the automated decisions, which include profiling, may lead to us deciding not to provide you with the requested Open Banking Services, either in relation to your specific request to use Open Banking Services, or in relation to your requests to use Open Banking Services over a set period of time, depending on the outcome of our fraud prevention assessment. For instance, we may assess the amounts and volumes of your transactions based on your selected account in relation to a Partner and whether your initiated payments in relation to a Partner were successfully executed. We will not make automated decisions about you that may significantly affect you unless (1) the decision is necessary as part of a contract that we have with you, (2) we have your explicit consent, or (3) we are required by law. In the United Kingdom, we may make such automated decisions where permitted by law (for example, where no special category data has been processed, and where other safeguards within UK privacy laws apply).

Your Privacy Rights

By law you may have a number of rights. You can submit requests under relevant laws to us via the details found in the "How to contact us" section below.

These rights may include to:

- **Request access to your Personal Information (commonly known as a data subject access request)**

This enables you to receive a copy of the Personal Information we hold about you and to check that we are lawfully processing it.

- **Require us to change incorrect or incomplete Personal Information**
- **Require us to delete or stop processing your Personal Information**

This enables you to ask us to delete or remove Personal Information where there is no good reason for us continuing to process it, you have withdrawn your consent, you have exercised your right to object to

processing and there are no overriding legitimate grounds for us to continue doing so, the Personal Information has been processed unlawfully or we are legally required to delete it. This does not apply e.g. where we need to process the data to establish, exercise or defend a claim.

- **Require the restriction of the processing**

In cases where the accuracy of your Personal Information is contested (for a period enabling us to verify the accuracy of the Personal Information), the processing is unlawful and you oppose our use of the data and ask it to be restricted, Where you have objected to the processing of your Personal Information and are awaiting our assessment of whether we have overriding legitimate grounds to continue processing it, or that we no longer need the Personal Information but you need it for legal claims purposes, you may ask for the restriction of the processing of such Personal Information. This means that Personal Information will, with the exception of storage, only be processed with your 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. Where processing is restricted, you will be informed before the restriction on processing is lifted.

- **Withdraw your consent (in the limited circumstances where you may have provided consent)**

You have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The withdrawal only affects future processing;

- **Object to the processing of your Personal Information**

You may object, on grounds relating to your particular situation, to processing which is based on the legitimate interests pursued by us or by a third party. In such a case, we will no longer process your Personal Information unless we have compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

- **Require data portability**

Where automated processing of your Personal Information is based on consent or the execution of a contract with you, you also have the right to data portability for information you provided to us – this means that you can obtain a copy of your Personal Information in a commonly used electronic format so that you can manage and transmit it to another data controller.

- **Lodge a complaint**

If you have any concerns about how we process your Personal Information, you are entitled to lodge a complaint. We encourage you to contact us first so we can address your concerns directly. Please contact us using the contact details below. You may also have the right to lodge a complaint with your local data protection authority. We take all complaints seriously and will respond as promptly as possible.

Generally, you will not have to pay a fee to access your Personal Information (or to exercise any of the other rights). However, where permitted by law, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. You may be required to verify your identity before we can respond to your request.

International Transfers

We may transfer your Personal Information between countries, including to countries which may not have similar privacy or data protection laws as your country of origin. However, we will always protect your information and transfer it in accordance with any applicable legal requirements for cross-border transfers of Personal Information. Where Personal Information is transferred to the United States from Europe, we will verify if the recipient ensures an adequate level of protection by participating in the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework and/or the UK-US Data Bridge. If this is not the case, or if Personal Information is otherwise transferred outside of the EEA, UK and/or Switzerland, we will ensure it is protected by other appropriate safeguards, such as Binding Corporate Rules, the EU Standard Contractual Clauses approved by the European Commission, the UK or Swiss Addendum to the EU's Standard Contractual Clauses, the UK's International Data Transfer Agreement or other legally permitted mechanisms. to ensure that the level of data protection afforded in the EEA, UK and/or Switzerland is not undermined. You may obtain a copy of such safeguards by using the contact details below.

Information Security

We take the security of your Personal Information seriously. We use physical, technical, organisational, and administrative safeguards to help protect your Personal Information from unauthorised access or loss. For example, we use encryption and other tools to protect sensitive information. Where we engage third parties to process Personal information on our behalf, they do so on the basis of written instructions and have a legal requirement to implement appropriate technical and organisational measures to ensure the security of Personal Information in compliance with the applicable data protection laws.

Changes to this Privacy Notice

We will make changes to this Privacy Notice from time to time. For example, we may make changes to this Privacy Notice to keep it up to date or to comply with legal requirements or due to changes in the way we operate our business. Any changes or updates we may make will be posted on our website so that you are aware of the impact to our data processing activities before you continue to engage with us. If we have your contact details on file we will notify you in advance of any significant changes. Please check back frequently to see the latest version on our website.

How to Contact Us

If you would like to exercise your privacy rights under relevant laws, please visit the [Privacy Rights Portal](#).

If you would like to contact the Data Protection Officer, please email privacy@visa.com.

For any other assistance, or to exercise your rights as an End User, you may contact us at the information below (*Please do not include sensitive information, such as your account number, in emails*):

If you are in Europe:

Email us: contact@tink.com

Write to us:

*Tink AB
Vasagatan 11
111 20 Stockholm, Sweden*

If you are in the UK:

Email us: contact@tink.com

Write to us:

*Tink Financial Services Limited
1 Sheldon Square
London, United Kingdom*