Privacy Notice – Visma Payments Oy - Visma Pay Application Service

Updated on 7th November 2024

General Information

This privacy notice describes the processing of personal data in connection with the use of the mobile application provided by Visma Pay. The purpose of this document is to help to understand what personal data we collect, why it is collected, and how we process, protect, store, and delete the personal data.

Data Controller and Contact Information

Visma Payments Oy acts as the data controller and is therefore responsible for obligations under data protection law. Inquiries related to processing should be sent to the contact person of the data controller.

Data controller: Visma Payments Oy
Business ID: 2486559-4
Address: Brahenkatu 4, 53100 Lappeenranta Finland
Website: https://www.visma.fi/vismapay/
Contact person: Mikko Rosengren mikko.rosengren@visma.com

Purpose and Basis of Personal Data Processing

Personal data is processed for the following purposes:

Processing Purpose	**Legal Basis**
• Managing customer relationships • Providing the service and functionalities of the application • Logging into the service • Providing customer service • Sending text messages to application users	Contract execution
• Designing and developing the application • Implementing and ensuring security and technical requirements • Transfer to Visma Connect for verifying the user's identity	Legitimate Interest: The data controller has a legitimate interest in developing and securing the application.
• Transfer the user's name, email, phone number, and address information to Mynt AB for concluding card agreements related to the application	Legitimate Interest: The client has a legitimate interest in increasing efficiency by using software to streamline receipt management.

Description of the Register's Content

Registered individuals are users of the Visma Pay application, from whom the following information may be stored:

- Basic personal details like the user's name, postal address, email address, and phone number
- Identification information such as social security number (The data controller stores the name, email address, and social security number during strong authentication.)
- Possible communication related to customer service
- Technical identifiers, such as IP address and device ID
- Payment information of the card linked to the application
- Receipt information linked to the application by the user

The data controller stores only the information necessary to execute the procedure.

Regular Sources of Information

The basic information stored in the register is primarily collected from the registered individual themselves. Additionally, identification information is automatically collected during customer authentication. Information is also stored when the customer contacts the data controller's customer service. We also collect device IDs, technical identifiers, and usage data directly from your mobile device, such as your phone.

By logging into the application and entering the required personal data, the customer agrees to the use of the data for the purposes described in the "Purpose and Basis of Personal Data Processing" section of this privacy notice.

Recipients of Personal Data

Personal data may be disclosed to companies within the same group and, on a case-by-case basis, or to authorities if there is a statutory basis for it.

Information may, if necessary, be disclosed within the Visma group to another Visma company, such as Visma Connect.

Additionally, the user's basic information is disclosed at the start of using the application to partner company Mynt AB, which issues credit cards that are integral to the service. This enables the functions required by the service and ensures a smooth user experience, as the application cannot be used without these cards.

Transfer of Personal Data Outside the EU/EEA

Personal data may be transferred outside the EU or the EEA to the extent permitted by law. In such situations, the data controller has ensured by necessary means that the data processor carrying out the transfer is able to commit to an adequate level of data security to ensure personal data protection:

- The European Commission has issued a decision on the adequacy of data protection in the respective country
- The contract concerning the transfer uses the standard contractual clauses approved by the European Commission

Rights of the Data Subject

The data subject has the right to obtain information about the collection and processing of personal data.

The data subject has the right to receive confirmation from the data controller of what information concerning them is stored in the register. The request must be sent in writing or electronically to the contact person of the data controller mentioned above. The data controller may charge a reasonable administrative fee if the data subject requests a copy more than once a year. The data controller may also charge a reasonable fee for fulfilling the request if the data subject's request is clearly unfounded or excessive.

The data subject has the right to have incorrect personal data concerning them rectified by the data controller without undue delay. Furthermore, the data subject has the right to have incomplete personal data completed.

The data subject has in certain situations the right to object to and restrict the processing of their personal data. If the processing of personal data is based on the data subject’s consent, they have the right to withdraw that consent at any time. Withdrawing consent may, however, affect the data subject's ability to continue using the services of the data controller. Withdrawal of consent does not affect the lawfulness of the processing of personal data by the data controller prior to the withdrawal.

In certain situations, the data subject also has the right to have the data controller delete information concerning them without undue delay (right to be forgotten).

If the data subject believes that the processing of their personal data is not lawful, they have the right to lodge a complaint with the supervisory authority.

Retention of Personal Data

Personal data is retained as long as necessary to fulfill the purposes of processing personal data described, unless otherwise required by law, after which the data is deleted. Personal data is stored for six (6) months from termination.

We retain personal data for an extended period only when required by mandatory legislation, legal claims against us, or relevant statutory or contractual time limits for claims or complaints.

Principles of Register Protection

The data controller ensures appropriate security through organizational, technical, and physical security measures, which comply with the security measures outlined in Article 32 of the GDPR,

considering the latest technology and implementation costs in relation to the risks associated with processing and the nature of the personal data to be protected.

When the data controller uses processors, the processing is agreed upon in a data processing agreement.

The data controller maintains adequate security measures to ensure that personal data is protected from destruction, alteration, and dissemination. Additionally, the data controller ensures that personal data is protected from unauthorized access and that data retrieval events are recorded and traceable.