Annex 1: Data Processing Agreement
Updated: 2025-11-28

1 AGREEMENT DOCUMENTS

References to the term "Processing Agreement" means this Annex 1, and the following appendices attached hereto:

Appendix 1	Services, Processing, Personal Data and Data Subjects
Appendix 2	Authorisation to engage Sub-processors

2 PURPOSE OF THE PROCESSING AGREEMENT

The purpose of the Processing Agreement is to regulate rights and obligations pursuant to applicable data protection legislation ("Data Protection Legislation") relating to the processing of "Personal Data" which means any information relating to an identified or identifiable natural person (the "Data Subject") which is processed by the Processor on behalf of the Controller. The Processing Agreement shall ensure that Personal Data is not used unlawfully and does not come into the possession of any unauthorized party.

3 SCOPE OF PROCESSING

The Controller determines the purposes and means of the processing of Personal Data. The Controller shall comply with its obligations pursuant to Data Protection Legislation, including responsibility to ensure necessary legal basis for collecting, processing and transfer of Personal Data.

The Processing Agreement concerns the Processor's processing of Personal Data on behalf of the Controller in connection with the Processor's provision of the "Services" as described in Appendix 1, Section 1.

The nature and the purpose of the processing, including operations and activities, are specified in Appendix 1, Section 2. The processing involves processing of such types of Personal Data as specified in Appendix 1, Section 3 of such categories of Data Subjects as specified in Appendix 1, Section 4.

The Processor, its Sub-processors, and other persons acting under the authority of the Processor who has access to the Personal Data shall process the Personal Data only on behalf of the Controller and in compliance with its documented instructions and in accordance with the Processing Agreement, unless otherwise stipulated in applicable statutory laws. The Processor shall inform the Controller of that legal requirement before processing, unless the statutory law prohibits such information on important grounds of public interest.

The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes the Data Protection Legislation.

4 CONFIDENTIALITY

The Processor, its Sub-processors, and other persons acting under the authority of the Processor who has access to the Personal Data are subject to a duty of confidentiality and shall observe professional secrecy in regard to the processing of Personal Data and security documentation pursuant to applicable Data Protection Legislation.

The Controller is subject to a duty of confidentiality regarding any documentation and information, received by the Processor, related to the Processor's and its Sub-processors' implemented technical and organisational security measures.

The confidentiality obligations also apply after the termination of the Processing Agreement.

5 INFORMATION SECURITY

The Processor shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by relevant supervisory authority pursuant to Data Protection Legislation to ensure an appropriate level of security.

The Processor shall assess the appropriate level of security and take into account the risks related to the processing, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

All transmissions of Personal Data between the Processor and the Controller or between the Processor and any third party shall be done by means of adequate encryption agreed between the parties.

The Processor shall provide the Controller with general descriptions of the Processor's and its Sub-processors' (to the extent that the Processor has access to such Sub-processors information) technical and organisational measures implemented to ensure an appropriate level of security.

The Processor shall provide reasonable assistance to the Controller, taking into account relevant information available to the Processor, if the Controller is obliged to perform an impact assessment and/or consult the supervisory authority in connection with the processing of Personal Data. The Controller shall bear any costs accrued by the Processor related to such assistance.

6 ACCESS TO PERSONAL DATA AND FULFILMENT OF DATA SUBJECTS' RIGHTS

Unless otherwise agreed or pursuant to applicable statutory laws, the Controller is entitled to access all Personal Data being processed by the Processor on behalf of the Controller. All costs and charges relating to any such access shall be for the account of the Controller, unless such access is available as a part of the Services.

The Processor shall assist the Controller for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights stipulated in Data Protection Legislation, including the Data Subject's right to (i) rectification of its inaccurate Personal Data; (ii) erasure of its Personal Data; (iii) restrict the processing of its Personal Data; and (iv) receive its Personal Data in a structured, commonly used and machine-readable format. The Processor shall be compensated for such assistance at the Processor's then current rates, unless otherwise agreed.

7 NOTIFICATION OF PERSONAL DATA BREACH

The Processor shall notify the Controller without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed ("**Personal Data Breach**"). The Controller is responsible for notifying the Personal Data Breach to relevant supervisory authority.

The notification to the Controller shall as a minimum describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences, in the reasonable opinion of the Processor, of the Personal Data Breach; (iii) the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, the Processor shall assist the Controller, including the provision, if available, of necessary contact information to the affected Data Subjects. The Controller shall bear any costs related to such assistance provided by the Processor and to such communication to the Data Subject. The Processor shall nevertheless bear such costs if the Personal Data Breach is caused by circumstances for which the Processor is responsible.

8 USE OF SUB-PROCESSORS

The Processor shall not engage another processor ("**Sub-processor**") in processing of the Personal Data without prior specific or general written authorisation of the Controller as stipulated in Appendix 2. The Processor shall inform the Controller of any intended changes concerning addition of replacement of any Sub-processors, and the Controller has the right to object to such changes.

The Processor shall ensure that its data protection obligations set out in the Processing Agreement and in Data Protection Legislation are imposed to any Sub-processors by a written agreement. Any Sub-processor shall in particular provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Legislation. The Processor shall remain fully liable to the Controller for the performance of any Sub-processor.

9 TRANSFER

Disclosure or transfer of Personal Data to countries outside EU/EEA may only occur in case of prior written approval from the Controller and is subject to EUs standard contractual clauses or other legal basis for such transfer or disclosure.

10 AUDITS

The Processor is obliged to provide the Controller with the documentation of implemented technical and organisational measures to ensure an appropriate level of security, and other information necessary to demonstrate the Processor's compliance with its obligations.

The Controller and the relevant supervisory authority shall be entitled to conduct security audits, including inspections and evaluation of Personal Data being processed, the systems used for this purpose, implemented technical and organisational measures, and Sub-processors.

The Controller is entitled to conduct security audits once a year. The Controller may appoint an external auditor to perform the security audits. The Controller shall bear any costs related to security audits initiated by the Controller.

11 TERM AND TERMINATION

The Processing Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller.

In the event of the Processor's breach of the Processing Agreement, the Controller may (i) instruct the Processor to stop further processing of Personal Data with immediate effect; (ii) terminate the Processing Agreement with immediate effect; and/or (ii) claim damages for direct economic loss caused by the Processor's breach, subject always to the provisions (including limitation of liability provisions) of the agreement(s) pursuant to which the Services are provided.

12 EFFECTS OF TERMINATION

The Processor shall, upon the termination of the Processing Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, unless otherwise stipulated in applicable statutory laws.

The Processor shall document in writing to the Controller that deletion has taken place in accordance with the Processing Agreement.

13 INDEMNIFICATION

The parties' liability for damage suffered by a data subject or other natural persons which is due to a violation of the General Data Protection Act (Regulation 2016/679), the General Data Act with regulations or other regulations that implement the General Data Protection Act, will follow the provisions of article 82 of the General Data Protection Act.

The limitation of liability in the Dintero Terms of Service Agreement applies for administrative fines imposed as a breach of the Data Protection Legislation.

14 NOTICES AND AMENDMENTS

All notices relating to the Processing Agreement shall be submitted in writing to the postal address or email address stated on the first page of the Processing Agreement.

Any modification or amendment of this Processing Agreement shall be effective only if agreed in writing and signed by both parties.

15 GOVERNING LAW AND LEGAL VENUE

This Processing Agreement shall be governed by Norwegian law. Legal venue is Oslo District Court.

Appendix 1: Processing, Personal Data, and Data Subjects

1. PROCESSING

The Personal Data will be subject to the following basic processing activities:

- The Controller and its employees can add and update their customers data.
- The Controller and its employees can search for their customers purchase and transaction data
- The Controller and its employees can download reports and other aggregated views and their content.
- Transactions done by the Controller's customers

2. PERSONAL DATA

The Personal Data processed concern the following type and categories, including any special categories of data:

- Personal details and contact information such as name, year of birth, gender, IP address, email address, telephone and place of residence
- Controllers customers and users activates such as spending, purchases, discount used, stamp cards used, payment, interests etc
- The Controller's personal identification number and bank account number as part of the transaction conducted by that customer

3. DATA SUBJECTS

The Personal Data processed concern the following categories of Data Subjects:

- Controller's customers
- Controller's users/employees

Appendix 2 – Authorisation to engage Sub-processors

The Processor is authorised to engage the following Sub-processor:

Provider	**Purpose**
Amazon Web Services	Cloud provider hosting our applications.
Visa Europe Limited	For processing Visa payments & services
Mastercard Europe SA	For processing Mastercard payments & services
3DSecure.io ApS	For 3DS/SCA
Swedbank Pay AB NUF	Processing Visa, Mastercard, Vipps, Swish, Apple Pay, Google Pay, Click 2 Pay & MobilePay transactions
Bambora AB	Processing Visa, Mastercard, Vipps, Apple Pay, Google Pay & MobilePay transactions
Vipps MobilePay AS	Processing Vipps transactions
Klarna Bank AB (publ)	Processing Klarna og Billie transactions
Collector Bank AB	Processing Walley transactions
Getswish AB	Processing Swish transactions
Kravia	Invoices
Strex AS	SMS Gateway
Mixpanel	For analytics of how users are using Dintero services
Stø AS	eID
DNB	Payouts
Creditsafe	Financial information
Hubspot	CRM

The Controller hereby grants a general written authorisation to the Processor to engage other Sub-processors provided that no Personal Data is transferred outside EU/EEA.

The Controller may from time to time provide optional/additional services and/or functionality to the Processor. Such optional services/functionality may be delivered by utilising Sub-processors and/or transfer of Personal Data outside EU/EEA. The Controller hereby grants a general written authorisation to engage such Sub-processors and approval of such transfer. Nevertheless, the Processor will provide the Controller with information related to the use of such Sub-processors and any transfer outside EU/EEA before the

Controller makes use of such optional services, and the the Parties shall cooperate in concluding appropriate legal basis for such transfer.