Contract on the commissioned processing

Personal Data

between

X1F GmbH
Borselstraße 20
22765 Hamburg

represented by

Sven Geilich
Stefan Mock

hereafter: **Client**

and

Sunday Group BV
Krommebeekpark 21
8800 Roeselare

represented by

Nies Vandecasteele

hereafter: **Contractor**

Version 1.1 from 17. August 2022

1 Introduction, Scope, Definitions

(1) This contract regulates the rights and obligations of the client and contractor (hereinafter referred to as "parties") in the context of the processing of personal data on behalf of the client.

(2) This contract applies to all activities in which employees of the contractor or subcontractors commissioned by him (subcontractors) process personal data of the client on his behalf.

(3) Terms used in this Agreement shall be understood as defined in the EU General Data Protection Regulation (GDPR). In this sense, the client is the "controller", the contractor is the "processor". Insofar as declarations must be made "in writing" in the following, the written form according to § 126 BGB is meant. In addition, declarations may also be made in another form, provided that appropriate verifiability is guaranteed.

2 Subject matter and duration of processing

2.1 Object

The contractor undertakes the following processing:

Worldwide distribution of the client's company fashion.

In doing so, the contractor processes personal data for the client within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of this contract.

The processing is based on the service contract XYZ existing between the parties (hereinafter referred to as the "Main Agreement").

2.2 Duration

The processing will commence on 24-07-2023 and will continue for an indefinite period of time until termination of this Agreement or the Main Agreement by either party.

The Client may terminate the Agreement at any time without notice if the Contractor has seriously violated data protection regulations or the provisions of this Agreement, if the Contractor is unable or unwilling to execute an instruction from the Client or if the Contractor refuses to exercise the Client's control rights in breach of contract. In particular, non-compliance with the obligations agreed in this contract and under Art. 28 GDPR constitutes a serious breach.

3 Type, purpose and data subjects of data processing

3.1 Type of processing (as defined in Art. 4 No. 2 GDPR)

The processing is of the following nature:

Collecting, storing, reading,, using, disclosing by transmission, or otherwise making available, alignment or combination, restriction, deletion or destruction of data

3.2 Purpose of the processing

The processing serves the following purpose:

The underlying purpose of the processing is regulated in the service description of the main contract.

3.3 Type of personal data (as defined in Art. 4 No. 1, 13, 14 and 15 GDPR)

The following data is processed:

- Name
- Address
- E-mail
- Cell phone number

3.4 Categories of data subjects (as defined in Art. 4 No. 1 GDPR)

The following are affected by the processing:

- employees of the client
- interested parties of the client

4 Obligations of the Contractor

(1) The Contractor shall process personal data exclusively as contractually agreed or as instructed by the Client, unless the Contractor is legally obliged to carry out specific processing (e.g. investigations by law enforcement or state security authorities). If such obligations exist for him, the contractor shall inform the client of these prior to processing, unless the notification is prohibited by law pursuant to Art. 28 para. 3 sentence 2 lit. a GDPR. Furthermore, the contractor does not use the data provided for processing for any other purposes, in particular not for its own purposes.

(2) The contractor confirms that he is aware of the relevant general data protection regulations. He observes the principles of proper data processing.

(3) The contractor undertakes to strictly maintain confidentiality during processing.

(4) Persons who may gain knowledge of the data processed on behalf of the company must undertake confidentiality in writing, unless they are already subject to a relevant duty of confidentiality by law.

(5) The contractor assures that the persons employed by him for processing have been familiarized with the relevant provisions of data protection and this contract before the start of processing. Appropriate training and awareness-raising activities shall be repeated on an appropriately regular basis. The Contractor shall ensure that persons employed for order processing are adequately instructed and monitored on an ongoing basis with regard to the fulfilment of data protection requirements.

(6) In connection with the commissioned processing, the contractor shall support the client as far as necessary in fulfilling its obligations under data protection law, in particular in the preparation and updating of the register of processing activities, in carrying out the data protection impact

assessment and a necessary consultation with the supervisory authority. The necessary information and documentation must be provided and forwarded to the client immediately upon request.

(7) If the client is subject to control by supervisory authorities or other bodies or if data subjects assert rights against him under Articles 12 to 22 GDPR , the contractor undertakes to support the client to the extent necessary insofar as the processing on behalf is concerned.

(8) The contractor may only provide information to third parties or the person concerned with the prior consent of the client. Inquiries addressed directly to him will be forwarded to the client immediately.

(9) The Contractor shall immediately draw the Client's attention to the Contractor if, in its opinion, an instruction issued by the Client violates statutory provisions (Art. 28 para. 3 sentence 3 GDPR). The contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the person responsible at the client after review.

(10) To the extent required by law, the contractor shall appoint a competent and reliable person as the data protection officer. It must be ensured that there are no conflicts of interest for the officer. In cases of doubt, the client can contact the data protection officer directly. The contractor shall immediately inform the client of the contact details of the data protection officer or justify why no officer has been appointed. Changes in the person or the internal tasks of the agent shall be communicated by the contractor to the client without delay.

(11) In principle, order processing takes place within the EU or the EEA. Any relocation to a third country may only take place with the consent of the client and under the conditions contained in Chapter V of the GDPR and in compliance with the provisions of this contract.

(12) As a matter of principle, the commissioned processing shall take place within the EU or the EEA. Any transfer to a third country may only take place with the consent of the Client and under the conditions contained in Chapter V of the General Data Protection Regulation and in compliance with the provisions of this contract.

5 Security of processing

(1) The data security measures described in Appendix 1 are defined as mandatory. They define the minimum owed by the contractor. The description of the measures must be so detailed that a competent third party can always see beyond doubt what the minimum owed should be on the basis of the description alone. No reference may be made to information that cannot be directly derived from this Agreement or its annexes.

(2) The data security measures can be adapted according to technical and organizational developments, as long as they do not fall below the level agreed here. The Contractor shall implement any changes necessary to maintain information security without delay. Changes must

be communicated to the client immediately. Significant changes are to be agreed between the parties.

(3) If the security measures taken do not or no longer meet the requirements of the client, the contractor shall notify the client immediately.

(4) The contractor assures that the data processed on behalf of the contractor will be strictly separated from other databases.

(5) Copies or duplicates will not be made without the knowledge of the client. Technically necessary, temporary duplications are excluded, insofar as an impairment of the level of data protection agreed here is excluded.

(6) The processing of data in private homes (mobile working or home office) is only permitted if the contractorensures that a level of data protection and data security in accordance with this contract is maintained and that the client's control rights specified in this contract are also fully exercised in the private homes concerned. can be exercised. The processing of data on behalf of private devices is only permitted with the prior written consent of the client in individual cases.

(7) Dedicated data carriers, which originate from the client or are used for the client, are specially marked and are subject to ongoing management. They must be stored appropriately at all times and must not be accessible to unauthorized persons. Inputs and outputs are documented.

(8) The Contractor shall provide regular proof of the fulfillment of its obligations, in particular the full implementation of the agreed technical and organizational measures as well as their effectiveness. The proof must be provided to the client at least every 12 months without being requested to do so and otherwise at any time upon request. Proof can be provided by approved codes of conduct or an approved certification process. Evidence must be kept at least until the expiry of three calendar years after the end of the order processing and must be submitted to the client at any time upon request.

6 Regulations for the correction, deletion and blocking of data

(1) The contractor will only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement made or in accordance with the instructions of the client.

(2) The contractor shall comply with the corresponding instructions of the client at any time and even after the termination of this contract.

7 Subcontracting relationships

(1) The commissioning of subcontractors is only permitted with the written consent of the client in individual cases.

(2) Consent is only possible if the subcontractor has been contractually imposed at least data protection obligations that are comparable to those agreed in this contract. Upon request, the client shall be granted access to the relevant contracts between the contractor and the subcontractor.

(3) It must also be possible to effectively exercise the rights of the client vis-à-vis the subcontractor. In particular, the client must be entitled to carry out inspections at any time to the extent specified herein, including at subcontractors, or to have them carried out by third parties.

(4) The responsibilities of the contractor and the subcontractor shall be clearly delineated.

(5) The Contractor shall carefully select the Subcontractor, with particular regard to the suitability of the technical and organizational measures taken by the Subcontractor.

(6) The forwarding of data processed on behalf of the subcontractor to the subcontractor is only permitted if the contractor has documented that the subcontractor has fully fulfilled its obligations. The contractor must submit the documentation to the client without being asked.

(7) The engagement of subcontractors who do not carry out processing on behalf exclusively from the territory of the EU or the EEA is only possible if the conditions set out in chapters 4 (10) and (11) of this contract are observed. In particular, it is only permissible if and as long as the subcontractor offers appropriate data protection guarantees. The contractor shall inform the client of the specific data protection guarantees offered by the subcontractor and how proof of this can be obtained.

(8) The contractor must adequately check compliance with the subcontractor's obligations on a regular basis, at the latest every 12 months. The test and its result must be documented in such a meaningful way that they are comprehensible to an expert third party. The documentation must be submitted to the client without being asked. The Contractor shall keep the documentation of tests carried out at least until the end of the third calendar year after completion of the order processing and shall submit it to the Client at any time upon request.

(9) If the subcontractor does not comply with its data protection obligations, the contractor shall be liable to the client for this.

(10) At present, the subcontractors specified in Appendix 2 with name, address and order content are engaged in the processing of personal data to the extent specified therein and approved by the client. The other obligations of the contractor towards subcontractors set out here remain unaffected.

(11) Subcontracting relationships within the meaning of this contract are only those services that are directly related to the provision of the main service. Ancillary services such as transport, maintenance and cleaning as well as the use of telecommunications services or user services are not included. The contractor's obligation to ensure compliance with data protection and data security in these cases remains unaffected.

8 Rights and obligations of the client

(1) The client is solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

(2) The client shall place all orders, partial orders or instructions in a documented manner. In urgent cases, instructions can be given orally. Such instructions shall be confirmed by the client without delay.

(3) The client shall inform the contractor immediately if he discovers errors or irregularities in the examination of the results of the contract.

(4) The Client is entitled to monitor compliance with the provisions on data protection and the contractual agreements at the Contractor's premises to an appropriate extent itself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site inspections. The persons entrusted with the inspection shall be granted access and insight by the contractor as far as necessary. The contractor is obliged to provide the necessary information, to demonstrate processes and to provide evidence that is necessary to carry out an inspection. The contractor is entitled to refuse inspections by third parties if they are in a competitive relationship with him or if there are similarly weighty reasons.

(5) Inspections at the contractor's premises must be carried out without avoidable disruptions to its business operations. Unless otherwise indicated for urgent reasons to be documented by the client, inspections shall take place after reasonable advance notice and during the contractor's business hours, as well as no more frequently than every 12 months. Insofar as the contractor provides proof of the correct implementation of the agreed data protection obligations as provided for in chapter 5 (8) of this contract, an inspection shall be limited to random sampling.

9 Notification obligations

(1) The Contractor shall notify the Client of any breaches of protection of personal data processed on behalf of the Client without undue delay. Justified suspicions of this must also be reported. The notification must be made at the latest within 24 hours of the contractor's knowledge of the relevant event to an address specified by the client. It shall contain at least the following information:

a. a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects, the categories concerned and the approximate number of personal data sets concerned;

b. the name and contact details of the data protection officer or other point of contact for further information;

c. a description of the likely consequences of the personal data breach;

d. a description of the measures taken or proposed by the contractor to remedy the personal data breach and, where appropriate, measures to mitigate its possible adverse effects;

(2) Also to be reported immediately are significant disruptions in the execution of the order as well as violations of data protection regulations or the provisions made in this contract by the contractor or the persons employed by him.

(3) The Contractor shall inform the Client immediately of any controls or measures taken by supervisory authorities or other third parties, insofar as these are related to order processing.

(4) The contractor assures that the client will be supported in its obligations under Art. 33 and 34 GDPR to the extent necessary.

10 Instructions

(1) The client reserves the right to issue comprehensive instructions with regard to processing on behalf of the client.

(2) The client and the contractor shall name the persons exclusively authorized to issue and accept instructions in Appendix 3.

(3) In the event of a change or long-term inability to attend the designated persons, the other party must be informed immediately of successors or representatives.

(4) The Contractor shall immediately draw the Client's attention to the Contractor if, in its opinion, an instruction issued by the Client violates statutory provisions. The contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the person responsible at the client.

(5) The contractor must document the instructions given to him and their implementation.

11 Termination of the order

(1) If, at the end of the contractual relationship, data processed in the order or copies thereof are still at the disposal of the contractor, the contractor shall, at the discretion of the client, either destroy the data or hand it over to the client. The choice must be made by the client within 2 weeks of the contractor's request. The destruction must be carried out in such a way that it is no longer possible to restore even residual information with reasonable effort. Physical destruction is carried out in accordance with DIN 66399. At least protection class 2 applies.

(2) The contractor is obliged to bring about the immediate destruction or return of subcontractors.

(3) The contractor must provide proof of proper destruction and submit it to the client without delay.

(4) Documentation that serves as proof of proper data processing must be kept by the contractor at least until the end of the third calendar year after the end of the contract. He can hand them over to the client for his relief.

12 Remuneration

The remuneration of the contractor is conclusively regulated in the main contract. There will be no separate remuneration or reimbursement of costs within the scope of this contract.

13 Liability

(1) The client and the contractor shall be jointly and severally liable for compensation for damages suffered by a person due to inadmissible or incorrect data processing within the scope of the contractual relationship.

(2) The contractor bears the burden of proof that damage is not the result of a circumstance for which he is responsible, insofar as the relevant data has been processed by him under this agreement. As long as this proof has not been provided, the contractor shall indemnify the client on first request against all claims asserted against the client in connection with the order processing. Under these conditions, the contractor shall also reimburse the client for all costs incurred in legal defense.

(3) The Contractor shall be liable to the Client for damages culpably caused by the Contractor, its employees or the persons commissioned by it with the execution of the contract or the subcontractors used by it in connection with the provision of the commissioned contractual service.

(4) Numbers (2) and (3) shall not apply if the damage was caused by the correct implementation of the commissioned service or an instruction issued by the client.

14 Penalty

(1) In the event of culpable breaches of its obligations under this contract, the contractor shall forfeit a contractual penalty appropriate to the breach. The contractual penalty shall be forfeited in particular in the event of deficiencies in the implementation of the agreed technical and organizational measures. In the case of permanent violations, each calendar month in which the infringement occurs in whole or in part shall be considered an individual case. The plea of continuation is excluded.

(2) The amount of the contractual penalty shall be determined by the client at its reasonable discretion. If it is not equitable, the determination shall be made by judgment.

(3) The contractual penalty is due upon declaration of its amount to the contractor.

(4) The contractual penalty has no influence on other claims of the client.

15 Special right of termination

(1) The Client may terminate the Main Agreement and this Agreement at any time without notice ("extraordinary termination") if there is a serious breach by the Contractor of data protection regulations or the provisions of this Agreement, if the Contractor is unable or unwilling to execute

a lawful instruction of the Client or if the Contractor refuses to exercise the Client's control rights contrary to the contract.

(2) A serious breach shall be deemed to exist in particular if the contractor does not or has not fulfilled the obligations specified in this agreement, in particular the agreed technical and organizational measures, to a significant extent.

(3) In the event of insignificant violations, the client shall set the contractor a reasonable deadline for remedial action. If the remedy is not provided in time, the client is entitled to extraordinary termination as described in this section.

(4) The Contractor shall reimburse the Client for all costs incurred by the Client as a result of the premature termination of the main contract or this contract as a result of extraordinary termination by the Client.

16 Other

(1) Both parties are obliged to treat as confidential all knowledge of trade secrets and data security measures of the other party obtained within the scope of the contractual relationship, even after the termination of the contract. If there is any doubt as to whether information is subject to the obligation of secrecy, it shall be treated as confidential until it has been approved in writing by the other party.

(2) If the Customer's property at the Contractor is endangered by measures taken by third parties (e.g. by seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor must notify the Customer immediately.

(3) For ancillary agreements, the written form and the express reference to this agreement are required.

(4) The defense of the right of retention within the meaning of § 273 BGB is excluded with regard to the data processed in the order and the associated data carriers.

(5) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

Signatures

Hamburg Place, date	Place, date
Client	Contractor

1. Appendix 1 – Technical and organizational measures

In the following, the order-related technical and organizational measures to ensure data protection and data security are defined, which the contractor must at least set up and maintain on an ongoing basis. The aim is to ensure in particular the confidentiality, integrity and availability of the information processed on behalf of the customer.

- Organization of information security: The contractor establishes and maintains a comprehensive framework for managing information security within their organization. This includes defining roles and responsibilities, creating policies and procedures, conducting risk assessments, and implementing security awareness programs.
- Personnel safety: The contractor ensures the physical safety and security of their personnel who have access to the customer's data. This includes measures such as access control to sensitive areas, and training employees on security protocols and best practices.
- Management of values: The contractor establishes and maintains a system for managing the values and principles that guide their information security practices. This includes promoting a culture of security awareness, ethics, and integrity throughout the organization.
- Access control: The contractor implements appropriate access controls to ensure that only authorized individuals can access the customer's data. This includes measures such as user authentication, role-based access control, and regular reviews of user access rights.
- Physical and environmental security:The contractor implements physical and environmental controls to protect the physical infrastructure and equipment that processes the customer's data. This includes measures such as secure data centers, video surveillance, fire suppression systems, and environmental monitoring.
- Reliability: The contractor ensures the reliability and availability of the systems and services that process the customer's data. This includes implementing redundancy and backup mechanisms, conducting regular system maintenance and testing, and having disaster recovery plans in place.
- Communication security: The contractor secures the communication channels used for transmitting the customer's data. This includes measures such as secure network configurations, encrypted communication protocols, and intrusion detection and prevention systems.
- Acquisition, development and maintenance of systems: The contractor follows secure practices throughout the lifecycle of systems used to process the customer's data. This includes conducting security assessments during system acquisition, implementing secure coding practices during development, and regularly updating and patching systems to address vulnerabilities.
- Supplier Relationships: The contractor establishes and maintains a process for managing the security of their third-party suppliers who have access to the customer's data. This includes assessing the security capabilities of suppliers, defining security requirements in contracts, and monitoring and auditing supplier compliance with security standards.
- Handling Information Security Incidents: The contractor establishes and maintains a process for handling information security incidents promptly and effectively. This includes procedures for identifying, reporting, and responding to security incidents, as well as mitigating the impact and preventing future incidents. The contractor should also have mechanisms in place for assessing the root cause of incidents and implementing necessary corrective actions.
- Information Security Aspects of Business Continuity Management: The contractor incorporates information security aspects into their business continuity management processes. This includes identifying critical information assets, assessing risks and vulnerabilities, developing incident response and recovery plans, conducting regular

testing and exercises, and continuously improving the resilience of systems and processes to ensure the timely restoration of services in the event of disruptions or disasters.

- Compliance: The contractor establishes and maintains a documented process for handling information security incidents promptly and effectively. This includes procedures for identifying, reporting, and responding to security incidents, as well as mitigating the impact and preventing future incidents. The contractor should also have mechanisms in place for assessing the root cause of incidents and implementing necessary corrective actions.

- Confidentiality (Art. 32 (1) (b) GDPR)
    - Access control: No unauthorized access to data processing systems
    - Access control: No unauthorized use of the system
    - Access control: No unauthorized reading, copying, modification or removal within the system
    - Separation control: Separate processing of data collected for different purposes
- Integrity (Art. 32 (1) (b) GDPR)
    - Transfer control: No unauthorized reading, copying, modification or removal during electronic transmission or transport
    - Input control: Determination of whether and by whom personal data has been entered, changed or removed from data processing systems
- Availability and resilience (Art. 32 (1) (b) GDPR)
    - Availability control: Protection against accidental or deliberate destruction or loss
    - Resilience control: Ability of the systems to deal with risk-related changes and have a tolerance and ability to compensate for disturbances
- Recoverability (Art. 32 (1) (c) GDPR)
- Procedures for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Kind. 25 para. 1 GDPR)
    - Data protection management: System for regular review, assessment and evaluation of data protection measures
    - Incident Response Management: System for preparing, identifying, and reporting security incidents
    - Privacy-friendly presets:
    - Order control:
    - Data protection supervisor

2. Appendix 2 – Authorized subcontractors

Company	Address	Contract content
BLECKMANN BELGIË NV	6/C Industriezone Kruisem9770 Belgium	Order fulfillment
MINICOLO COMM. V.	A. Stocletlaan 228 Duffel2570 Belgium	Server provider

3. Appendix 3 – Persons authorized to issue instructions, address for reporting data breaches

The following persons are authorized to issue instructions:

Hendrik Dold
Director Corporate Communications
hendrik.dold@x1f.one

Katharina Godo
Corporate Communications Specialist
katharina.godo@x1f.one

Sven Geilich
COO / Managing Partner
sven.geilich@x1f.one

Stefan Mock
CIO / Managing Partner
stefan.mock@x1f.one

Zoran Tepsic
CFO / Managing Director
zoran.tepsic@x1f.one

The following persons are authorized to receive instructions:

Niels Vandecasteele
CEO
Niels.vandecasteele@teamsunday.com

Sofie Snauwaert
Business Process Manager
sofie.snauwaert@teamsunday.com

Contact for personal data breach notifications:

Sebastian Raguse
Data Protection Manager / X1F Data Protection Officer
datenschutz@x1f.one

In the event of a change or long-term inability to contact persons, the contractual partner must be informed immediately and, in principle, in writing or electronically of the successors or representatives. The instructions shall be kept for their period of validity and thereafter for three full calendar years.

4. Appendix 4 – Data Protection Officer

Currently, no data protection officer has been appointed to the contractor.