

Data protection agreement for commissioned data processing in accordance with Article 28 of the EU General Data Protection Regulation (GDPR)

On behalf of

hereinafter referred to as "**controller**"

processed by

fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

hereinafter referred to as "**processor**"

§1 General

- (1) The processor processes personal data on behalf of the controller within the meaning of Article 4 (8) and Article 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). This data protection agreement governs the rights and obligations of the parties in connection with the processing of personal data.
- (2) This data protection agreement specifies the obligations of the processor and the controller (hereinafter also referred to as the "Parties") with regard to data protection arising from the service agreement/SLA/main contract/order (hereinafter referred to as the "service agreement").
- (3) The terms used in this contract are to be understood in accordance with their definition in the GDPR.

§2 Contract content

The subject matter, type and purpose of the commissioned processing as well as the categories of personal data processed and the type of data subjects affected by the data processing are set out in the service agreement and in Annex 1 to this agreement.

§3 Duration of the processing of personal data

The duration of this contract corresponds to the term of the service agreement, unless the following provisions provide for additional obligations or cancellation rights. However, the contract shall apply for as long as the processor processes personal data of the controller.

§4 Instructions

- (1) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.
- (2) The controller's instructions are defined by the service agreement, this contract and its annexes and may also be amended, supplemented or replaced by the controller in writing or in a documented electronic format by individual instructions. The controller is authorised to issue corresponding instructions at any time. This includes instructions regarding the type, scope and procedure of data processing as well as with regard to the correction, deletion and blocking of data. Changes to the object of processing and procedural changes must be jointly agreed and documented.
- (3) Instructions that go beyond the service agreed in the main contract shall be treated as a request for a change in service. Regulations on any compensation for additional expenses incurred as a result of supplementary instructions from the controller to the processor shall remain unaffected.
- (4) The processor's persons authorised to receive instructions are listed in Annex 1. In the event of a change or a longer-term absence of the named persons, the successor or representative must be named to the contractual partner immediately in text form.
- (5) All instructions issued must be documented by both the controller and the processor and retained for the duration of their validity and subsequently for a further three full calendar years. Instructions that go beyond the service agreed in the main contract shall be treated as a request for a change in service. This shall be without prejudice to any provisions on compensation for additional expenses incurred as a result of additional instructions issued by the controller to the processor.
- (6) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions. The processor shall be entitled to suspend the implementation of the instruction in question until it is confirmed or amended by the

controller. The processor may refuse to carry out any obviously unlawful instructions.

§5 Processing obligations of the processor

- (1) The processor confirms that it has appointed a data protection officer in accordance with Article 37 GDPR and that he monitors compliance with data protection and data security regulations with the involvement of the data protection officer. The controller shall be informed of the data protection officer's contact details in Annex 1. The controller must be informed immediately of any change of data protection officer.
- (2) The processor undertakes to maintain confidentiality when processing the controller's personal data in accordance with the contract. This obligation shall continue to apply after termination of the contract. In particular, the processor warrants that it will familiarise its employees employed to carry out the work with the data protection provisions applicable to them before they commence their work. Furthermore, the relevant employees shall be bound to confidentiality in an appropriate manner for the duration of their work and also after termination of the employment relationship. The employees must be instructed about the special data protection obligations arising from this contract as well as the existing instruction and purpose limitation.
- (3) The processor is obliged to implement and comply with all technical and organisational measures necessary for this processing in accordance with Article 32 GDPR. Details are regulated in § 10 of this agreement.
- (4) The controller gives its express consent that employees of the processor may also perform the data processing associated with this order processing outside the processor's premises, e.g. by teleworking, home office, mobile working. The prerequisite for this is that
 - a) the technical and organisational measures agreed in this contract for the processing situation (see Annex 2) are guaranteed;
 - b) and that, if data of the controller is processed in a private residence, the processor shall take appropriate measures to ensure that the requirements of the GDPR are observed.
- (5) The technical and organisational protective measures taken by the Processor in accordance with Article 32 GDPR for the deployment of employees of the Processor in the context of teleworking, home office and mobile working are attached as Annex 2. Changes to the measures taken by the Processor are permitted under certain conditions specified in § 10 of this agreement.
- (6) The processor undertakes to regularly monitor the internal processes to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection laws and that the protection of the rights of the data subject is guaranteed.

§6 Cooperation and support obligations of the processor

- (1) If a data subject asserts rights under Chapter III GDPR (access, rectification or erasure of their data) directly against the processor, the processor shall not respond independently. The processor shall immediately refer the data subject to the controller and await the controller's instructions.
- (2) Where possible, the processor shall support the controller with suitable technical and organisational measures in fulfilling the controller's obligations under Article 12 to 22 GDPR. To this end, the processor shall provide the controller with all necessary information, provided that this does not violate the processor's confidentiality obligations towards third parties.
- (3) The processor may only provide information to third parties or the data subject with the prior consent of the controller.
- (4) The processor is obliged to support the controller in complying with the obligations set out in Article 32 to 36 GDPR to the extent necessary.
- (5) The processor shall support the controller in drawing up the record of processing activities in accordance with Article 30 GDPR and shall provide the necessary information upon request.
- (6) The processor undertakes to ensure the verifiability of the fulfilment of the obligations under this data protection agreement and under the applicable data protection regulations and to make the corresponding evidence available to the controller upon request.
- (7) The processor undertakes to support the controller in an appropriate manner in the fulfilment of its control obligations within the framework of the order control, as described in § 11 of this agreement, and to make the necessary resources available.

§7 Information obligations of the processor

- (1) The processor shall immediately notify the controller of a personal data breach concerning data processed by the processor. This also applies in particular with regard to any reporting and notification obligations of the controller in accordance with Article 33 and 34 GDPR.
- (2) The personal data breach notification shall contain the following information as far as possible:
 - a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
 - b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

- (3) The processor shall immediately take the necessary measures to secure the data and to minimise possible adverse consequences for the data subject(s), inform the controller thereof and request further instructions from the controller.
- (4) The processor warrants that it will provide the controller with appropriate support in fulfilling its obligations under Article 33 and 34 GDPR where necessary. The processor may only carry out notifications for the controller in accordance with Article 33 or 34 GDPR following prior instruction.

§8 Use of sub-processors

- (1) The processor has the controller's general authorisation for the engagement of sub-processors in compliance with the following provisions.
- (2) The commissioning of additional processors is only permitted if the processor informs the controller of the name and address of the sub-processor and the intended activities of the sub-processor. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (3) The processor may engage new subcontractors or replace existing ones, provided that the processor notifies the controller of the planned changes in advance in writing or in text form, giving the controller the opportunity to object to such changes. Authorisation shall be deemed to have been granted if the controller does not object to an intended change within two weeks of notification.
- (4) In the event of an objection, the processor may, at its own discretion, either
 - a) provide the service without the intended change or,
 - b) if the provision of the service is not reasonable for the processor without the intended change, discontinue the service affected by the change within a reasonable period of time and prior notification of the controller.

The processor shall immediately inform the Controller of the intended cessation and deadline (text form is sufficient). In this case, both parties shall be granted the separate

right of cancellation within 2 weeks of notification of the discontinuation.

- (5) At the time the contract is concluded, the subcontractors specified in Annex 3 with their name, address, contract content and processing location are engaged in the processing of personal data for the processor to the extent specified therein. The controller hereby agrees to their commissioning. If the listed subcontractors have processing locations in third countries, the controller agrees to the transfer of data to these third countries, provided that the provisions of § 9 of this agreement are complied with.
- (6) Services that the processor utilises from third parties as an ancillary service to support the execution of the order are not to be understood as subcontracting relationships within the meaning of this regulation. These include, for example, postal, transport and dispatch services, cleaning services, telecommunication services with no specific connection to services provided by the processor for the controller and security services.
- (7) Maintenance and testing services constitute subcontractor relationships requiring consent if they are provided for IT systems that are also used in connection with the provision of services for the controller. The processor is nevertheless obliged to ensure that appropriate precautions and technical and organisational measures are taken to guarantee the protection of personal data, even in the case of ancillary services provided by third parties.

§9 International data transfers

- (1) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
- (2) The controller agrees that where the processor engages a sub-processor in accordance with § 8 for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by invoking the existence and applicability of an adequacy decision, using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met or the sub-processors have demonstrably submitted to approved codes of conduct.

§10 Technical and organisational measures

- (1) The processor shall design the internal organisation in its area of responsibility in such a way that it meets the special requirements of data protection and ensures that it has taken all necessary technical and organisational measures to adequately protect the data of the controller in accordance with Article 32 GDPR.

- (2) In Annex 2, the technical and organisational measures appropriate to the identified risk are presented in detail, taking into account the state of the art protection objectives and paying particular attention to the IT systems and processing procedures used by the processor.
- (3) The technical and organisational measures are subject to progress and further development. The processor reserves the right to change the security measures taken, whereby it shall ensure that the contractually agreed level of protection is not fallen short of. Any changes made must be documented in any case. The current version of the technical and organisational measures must be made available to the controller on request.
- (4) The processor must coordinate significant changes with the controller in documented form (in writing, electronically). Such agreements must be retained for the duration of this contract.

§11 Control rights of the controller

- (1) The controller shall have the right to carry out commissioned inspections of the processor in consultation with the processor. The controller shall have the right to verify compliance with this agreement and the applicable data protection regulations by the processor in its business operations by means of inspections, of which the processor must generally be notified in advance. The processor undertakes to assist with these audits where necessary and to provide the necessary information and evidence upon request.
- (2) The controller is authorised to have the checks carried out by an external auditor commissioned by the controller at its own expense, provided that the external auditor is not in a competitive relationship with the processor or there are no other legitimate reasons on the part of the processor to the contrary. The processor shall be entitled to obtain the name of the external auditor and evidence of the auditor's confidentiality obligations in advance.
- (3) With regard to the controller's monitoring obligations pursuant to Article 28 (1) GDPR before the start of data processing and during the term of the contract, the processor shall ensure that the controller can verify compliance with the technical and organisational measures taken at any time by means of on-site inspections. It is agreed that the number of on-site inspections without occasion shall be limited to once a year. Inspections without cause must be notified in good time and carried out in such a way that the processor's operational processes are not disproportionately disrupted. Any costs incurred shall be borne by the respective contracting parties themselves. For inspections beyond this without cause, remuneration shall be agreed by the controller in accordance with the actual costs incurred by the processor.
- (4) The processor can also provide evidence of the implementation of the technical and organisational measures in accordance with Article 32 GDPR by submitting a current certificate or report (e.g. auditor, audit). Other options for providing proof are a current certification (e.g. in accordance with ISO/IEC 27001) or a data protection seal or certification

mark in accordance with Article 42 GDPR or the submission of a data protection or IT security concept that meets the requirements of the GDPR. The controller reserves the right to carry out further checks after reviewing the evidence provided.

- (5) If proof of compliance with the provisions of the GDPR is provided by the processor with the help of a certification pursuant to Article 42 GDPR, the processor undertakes to inform the controller immediately of the revocation of a certification pursuant to Article 42 (7) GDPR.

§12 Deletion and return of personal data

- (1) After completion of the processing or earlier at the request of the controller, but at the latest after termination of this contract, the processor shall hand over to the controller all documents, processing or utilisation results and data files relating to the contractual relationship that have come into its possession. Alternatively, the data in question may be deleted or destroyed in accordance with data protection regulations following prior consent. The same applies to test and scrap material. This obligation also applies to the same extent to sub-processors. Data and copies required for the fulfilment of liability and warranty claims remain unaffected. The deletion log must be submitted on request.
- (2) Documentation that serves as proof of proper data processing in accordance with the contract or may not be deleted for legal reasons, e.g. due to statutory retention obligations, must be retained by the processor beyond the end of the contract in accordance with the respective retention periods. After the retention period has expired, they must be securely deleted immediately. The controller shall be informed of the type and scope of the data remaining with the processor, unless prohibited to do so by Union or Member State law. The processor may hand over this data to the controller at the end of the contract in order to relieve the controller.

§13 Liability

- (1) Processors and controllers are liable externally in accordance with Article 82 (1) GDPR for material and immaterial damage suffered by a person due to a breach of the GDPR or this DPA. In the internal relationship, the processor and controller are liable in accordance with their respective share of causation and fault. If, in such a case, a person makes a claim for damages against one party in whole or in part, this party may demand indemnification or hold harmless from the other party to the extent that this corresponds to its share of causation and fault.
- (2) The processor shall be liable to the controller for culpable breaches of this agreement in accordance with the statutory provisions.
- (3) The processor shall be liable to the controller for the fault of a sub-processor commissioned by the processor as for its own fault. If the sub-processor fails to fulfil its data protection obligations, the processor shall be liable to the controller for the subcontractor's compliance

with its obligations.

§14 Contract term and cancellation

- (1) The contractual relationship enters into force upon signature by both contracting parties and runs for as long as the main contract. The ordinary right of cancellation corresponds to that of the main contract.
- (2) If the basis for the fulfilment of the contract is significantly changed or ceases to exist entirely due to a change in the legal or statutory situation or an intervention or other measure by the supervisory authorities, both parties are entitled to an adjustment of the contract to the new circumstances, insofar as this is possible and reasonable for both parties. If an adjustment to the contract is not possible or is unreasonable for one party, this shall constitute good cause for extraordinary cancellation for both parties.

§15 Confidentiality

The parties undertake to treat as confidential all knowledge of trade and business secrets and data security measures of the other party obtained in the course of the order processing. Trade and business secrets are all facts, circumstances and processes relating to the company of one of the parties which are not in the public domain but are only accessible to a limited group of persons and which the party concerned has a legitimate interest in not disclosing. Data security measures are all technical and organisational measures within the meaning of Article 32 GDPR that a party has taken. This confidentiality obligation shall continue to apply after termination of this contract.

§16 Final provisions

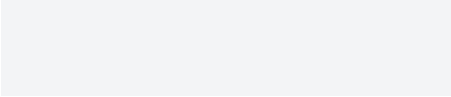
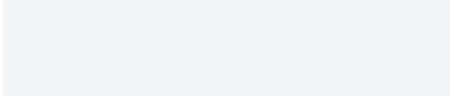
- (1) Should one or more provisions of this contract be or become invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by a valid one that comes closest to the original economic purpose and is permissible under applicable law.
- (2) Amendments and additions to this agreement, the respective individual contract and all its components must be made in writing. This also applies to the waiver of this formal requirement.
- (3) For all disputes arising from or in connection with this contract, the jurisdiction agreement of the main contract shall apply - insofar as permissible.
- (4) The annexes attached to the contract form an integral part thereof.

Annexes to the contract

Annex 1: Specification of the subject matter of the order

Annex 2: Technical and organizational measures for data protection

Annex 3: List of sub-processors

 fynk GmbH Signatur ausständig	 Kunde Signatur ausständig
--	---