

Asset Tracker

Attachment DPA for test package



A Vodafone Company

Data processing agreement (DPA)

This agreement has been comprehensively drawn up and contains all information in accordance with Art. 28 DSGVO between the client as Controller and grandcentrix as Processor.

Preamble

The processor processes personal data of the controller. The Parties agree that the provisions of the EU General Data Protection Regulation (GDPR), in particular the provisions on data processing by order, shall apply to this Agreement. The Processor declares that it is able to properly perform the commissioned services in accordance with Art. 28 GDPR.

The agreement regulates the data protection measures within the meaning of Art. 28 GDPR and the rights and obligations of the Controller and the Processor to fulfill the data protection requirements.

This agreement is based on the service contract in accordance with the Asset Tracker test package order form.

| | |
|---|---|
| <p>§ 1 Subject and duration of the order</p> <p>(1) The subject matter of the order is set out in the associated order form - Asset Tracker.</p> <p>(2) The duration and term of the order shall result from the specified service contract unless other terms are specified here.</p> <p>(3) The possibility of termination without notice remains unaffected. The controller may terminate the agreement at any time without notice if there is a serious breach by the processor of the applicable data protection regulations or of obligations under this agreement, the processor is unable or unwilling to carry out instruction of the controller.</p> <p>§ 2 Nature and purpose of processing</p> <p>(1) The nature and purpose of the processing are subject to instructions and are based on the above-mentioned service agreement.</p> <p>§ 3 Nature of personal data and categories of data subjects</p> <p>(1) Data processing concerns the following categories of natural persons: Employees, customers and third parties defined by the customer whose data is transmitted.</p> <p>§ 4 Types of personal data</p> <p>(1) Data processing includes the following personal data/operational data and categories of data: Contact data and master data of the Controller required to establish, execute and, if necessary, terminate the existing contractual relationship; Traffic data (data processed in the provision of a telecommunications service); tracking device data, i.e. information transmitted by the tracking devices (e.g. log files, system states, configurations, usage data); Location data from network communication, i.e. cell IDs from mobile connections, GPS coordinates, etc....</p> <p>§ 5 Authority of the Controller to issue instructions</p> <p>(1) The data shall be processed exclusively within the framework of the agreements made and in accordance with the instructions of the Controller. The instructions shall be issued in writing. Verbal instructions shall be confirmed in writing without delay. The instructions shall be retained for the duration of the contractual relationship and at least for the duration of the post-contractual obligations.</p> <p>(2) Persons authorized to issue instructions on behalf of the Controller and recipients of instructions at the Processor must be named. Changes to the person authorized to issue instructions or the recipient of instructions must be communicated immediately.</p> <p>(3) Changes to the processing object and procedural changes must be jointly agreed and documented.</p> | <p>§ 6 Safeguarding confidentiality and other secrets</p> <p>(1) The Processor may only use personal and other data or information of which it becomes aware in the course of fulfilling this contract for the purposes of the commissioned service. The Processor undertakes to maintain the confidentiality and integrity of the personal data and to treat all personal data and other internal company circumstances, data and information (trade secrets) of which it becomes aware in connection with the acceptance and execution of the order as confidential and to oblige the employees working within the scope of this contract to maintain confidentiality even after the termination of the employment relationship and to instruct them about the data protection obligations arising from this contract, the fact that the processing of the data is subject to instructions and its purpose limitation. This confidentiality obligation shall also apply beyond the termination of the contractual relationship.</p> <p>(2) The Processor confirms that it is aware of the relevant data protection regulations. The Processor warrants that it will familiarize the employees involved in the execution of the order with the data protection provisions applicable to them.</p> <p>(3) The Processor undertakes to observe all other secrets, insofar as these are relevant to the processing, such as social secrecy, telecommunications secrecy and other professional secrets in accordance with Section 203 of the German Criminal Code (StGB), as well as to oblige and instruct employees to ensure that these secrets are kept.</p> <p>(4) The Processor is obliged to keep secret all knowledge of the Controller's administrative access data and data security measures obtained within the scope of the contractual relationship and not to disclose them to third parties under any circumstances. The Processor may only make use of the access rights granted to it to the extent necessary to carry out the data processing. The obligation to maintain confidentiality and other secrets shall also apply beyond the termination of this contract.</p> <p>(5) The above obligation shall not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain confidentiality or which is publicly known.</p> |
|---|---|

Asset Tracker

Attachment DPA for test package



A Vodafone Company

| | |
|--|---|
| <p>§ 7 Obligations of the Processor</p> <p>(1) Processing obligations The Processor shall carry out the order exclusively within the framework of the agreements made and in accordance with the Controller's instructions. The Processor shall not use the data for any other purposes and, in particular, shall not be entitled to pass it on to third parties. Extracts, copies or duplicates of data or data carriers may only be produced and used without the Controller's knowledge if this is necessary for the execution of the order or to ensure proper data processing or if there is a legal or other obligation to retain data. Any extracts, copies or duplicates made shall be securely deleted or destroyed by the Processor in accordance with data protection regulations or handed over to the Controller immediately after completion of processing or use. The Processor undertakes to only use software, data or data carriers that have been reliably checked for the absence of malware.</p> <p>(2) Duty to inform In the event of a disruption in processing or a data breach, the Processor shall immediately initiate all appropriate and necessary measures to secure the data and to minimize any damage to the data subjects and the Controller. The Processor undertakes to:</p> <ul style="list-style-type: none"> - To inform the Controller immediately, but at the latest within 36 hours, of any breaches of regulations on the protection of personal data or of the provisions of this agreement, to provide all necessary information and to support the clarification of such incidents as far as possible. Data protection breaches include in particular the loss of confidentiality and the loss or destruction or falsification of the Controller's data or other confidential information within the meaning of this contract. - not to provide information to third parties or inquiries from affected persons, or only to do so in accordance with the Controller's instructions. Requests from affected persons must be forwarded to the Controller immediately. - to provide information to employees of the Controller only to authorized persons. - To inform the Controller about inspections by the data protection supervisory authority, in particular pursuant to Art. 58 GDPR, and about any measures and requirements for the protection of personal data. - To support the Controller in fulfilling its obligations with regard to the rights and requests of data subjects to an appropriate extent. <p>(3) Organizational duties Data protection incidents and other security-relevant disruptions to processing must be documented, including their effects and the remedial measures taken, and reported to the Controller. The documentation shall be made available to the Controller without delay. The Processor shall inform the Controller of the name and contact details and any changes in the person of the company data protection officer.</p> <p>Data Protection Officer: Volker Leniger Mail: datenschutzbeauftragter@grandcentrix.net Phone: +49 (221) 677 860 - 70</p> <p>(4) Violation of instructions against data protection law The Processor shall inform the Controller immediately if it believes that an instruction violates the GDPR or other data protection regulations. The Processor may suspend the execution of the instruction until confirmation by the Controller. The Controller shall be liable for unlawful instructions and shall indemnify the Processor against claims for damages and other claims in this respect.</p> | <p>§ 8 Obligations to cooperate and provide support</p> <p>(1) The Processor shall ensure a level of protection of personal data adequate to the risk to the rights and freedoms of the data subjects. To this end, the Processor undertakes to design and continuously update its internal organization and the necessary technical and organizational measures, taking into account the respective state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing and the different probability of occurrence and severity of the risk to the rights and freedoms of the data subjects, in such a way that they meet the special requirements of data protection pursuant to Art. 32 GDPR and guarantee the protection of the rights of the data subjects. The security level of the defined measures must not be undercut. See Annex 1</p> <p>(2) Inquiries from data subjects regarding their rights or information, corrections or deletions of data requested by a data subject shall be forwarded immediately by the Processor to the Controller for processing. Information to third parties or data subjects may only be provided on the instructions of the Controller or must be forwarded to the Controller for processing.</p> <p>(3) In the event of a personal data breach, the Processor shall document the incident and support the Controller in fulfilling the obligation to notify the supervisory authority in accordance with Art. 33 GDPR and the obligation to notify data subjects in accordance with Art. 34 GDPR.</p> <p>(4) The Processor undertakes to support the Controller in the risk identification and subsequent data protection impact assessment as well as in any necessary prior consultation in accordance with Art. 35 and 36 GDPR.</p> <p>(5) The Processor undertakes, within the scope of Art. 28 GDPR, to provide the information required for the register of processing activities and for the risk identification and any data protection impact assessment without delay and insofar as it concerns its area of responsibility.</p> <p>§ 9 Subcontracting relationships</p> <p>(1) The Controller agrees that the Processor may involve subprocessors. The contractual services or partial services shall be performed with the involvement of the listed subprocessors. See Annex 2</p> <p>(2) Inquiries from data subjects regarding their rights or information, corrections and deletions of data requested by a data subject shall be forwarded immediately by the Processor to the Controller for processing. Information to third parties or data subjects may only be provided on the instructions of the Controller or must be forwarded to the Controller for processing.</p> <p>(3) In the event of a personal data breach, the Processor shall document the incident and support the Controller in fulfilling the obligation to notify the supervisory authority in accordance with Art. 33 GDPR and the obligation to notify data subjects in accordance with Art. 34 GDPR.</p> <p>(4) The Processor undertakes to support the Controller in the risk identification and subsequent data protection impact assessment as well as in any necessary prior consultation in accordance with Art. 35 and 36 GDPR.</p> <p>(5) The Processor undertakes, within the scope of Art. 28 GDPR, to provide the information required for the register of processing activities and for the risk identification and any data protection impact assessment without delay and insofar as it concerns its area of responsibility.</p> |
|--|---|

Asset Tracker

Attachment DPA for test package



A Vodafone Company

§ 10 Control and audit rights of the Controller

- (1) The Controller is solely responsible for assessing the permissibility of the processing of personal data and for the implementation of the rights of the data subjects. In the case of commissioned data processing, the Controller shall, in accordance with Art. 28 para. 1 sentence 1 GDPR, only work with processors who offer sufficient guarantees that appropriate technical and organizational measures have been implemented to meet the requirements of the GDPR.
- (2) The Controller shall be authorized, after prior consultation/notification, to check compliance with the data protection regulations and the contractual agreements, in particular the technical and organizational measures taken by the Processor, during normal business hours without disrupting operations to the extent necessary.
- (3) The rights of the Controller shall continue to exist during the term of this agreement and beyond until the claims arising from this agreement become time-barred.

§ 11 Procedure after completion of the order

- (1) After completion of the processing, at the latest after termination of this contract, the Processor shall hand over to the Controller all documents and processing or usage results that have come into its possession or personal or other confidential data produced or copied in connection with the contractual relationship or destroy or securely delete them in accordance with data protection regulations in consultation with the Controller.
Upon termination of this contract, the Processor shall confirm to the Controller in writing the secure deletion or secure destruction of all documents in its possession.
This obligation shall also apply to the same extent to any subprocessors engaged. Data whose deletion is not possible for technical reasons or would cause a disproportionately high effort, as well as copies that are necessary to prove the correctness of data processing or to fulfill liability and warranty claims, remain unaffected.

- (2) Processing of this data must be restricted in accordance with Art. 18 GDPR. The data may be stored by the Processor beyond the end of the contract in accordance with the respective retention periods and must be securely deleted immediately after expiry of the retention period. The Controller must be informed of the type and scope of this stored data. The Processor may hand over this data to the Controller at the end of the contract in order to relieve the Controller.

§ 12 Effectiveness of the agreement

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

§ 13 Liability

Liability is governed by the provisions of Art. 82 GDPR.

Appendix 1:

(detailed description for data with a higher assessed risk)
Description of the agreed technical and organizational measures

Appendix 2:

Subprocessor

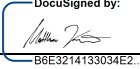
Signature of the Controller:

| |
|------------------------------|
| Company: |
| Place, date: |
| Signature of the Controller: |
| Name in block capitals: |

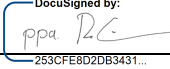
Signature of the Controller:

| |
|------------------------------|
| Company: |
| Place, date: |
| Signature of the Controller: |
| Name in block capitals: |

Signature grandcentrix:

| |
|---|
| Company: grandcentrix GmbH |
| Place, date: Köln, 24.05.2024 15:04 CEST |
| Signature of the Processor:  |
| Name in block capitals: Matthias Krömer |

Signature grandcentrix:

| |
|---|
| Company: grandcentrix GmbH |
| Place, date: Köln, 23.05.2024 00:22 PDT |
| Signature of the Processor:  |
| Name in block capitals: Raphael Heinrich |

Asset Tracker

Attachment DPA for test package



A Vodafone Company

Appendix 1

(detailed description for data with a higher assessed risk)

Description of the agreed technical and organizational measures

In accordance with Art. 28 para. 1 GDPR, the controller only works with processors who offer sufficient guarantees that appropriate technical and organizational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR and the protection of the rights of the data subjects is guaranteed.

| | |
|--|---|
| <p>Encrypted data storage</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Encrypted hard disks and mobile data carriers <input checked="" type="checkbox"/> Encryption during transmission <input checked="" type="checkbox"/> Encrypted e-mail transmission <input checked="" type="checkbox"/> Data exchange via https connection <input checked="" type="checkbox"/> Encryption of networks <p>VPN connection</p> <p>Access control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Electronic access transponders <input checked="" type="checkbox"/> Access authorization concept <input checked="" type="checkbox"/> Video surveillance (main entrance when ringing) <input checked="" type="checkbox"/> Accompaniment of visitor access by own employees <input checked="" type="checkbox"/> Graded security areas and controlled access <input checked="" type="checkbox"/> Separately secured access to the data center <input checked="" type="checkbox"/> Storage of the servers in locked rooms <input checked="" type="checkbox"/> Alarm system in the data center <p>Access control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Password protection for computer workstations <input checked="" type="checkbox"/> Use of individual passwords <input checked="" type="checkbox"/> Password policy with minimum requirements for password complexity <input checked="" type="checkbox"/> Process for assigning rights when new employees join the company <input checked="" type="checkbox"/> Process for withdrawing rights when employees leave the company <input checked="" type="checkbox"/> Obligation to maintain confidentiality <p>Functional and/or time-limited assignment of user authorizations</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Automated blocking of accounts after multiple incorrect password entries <p>Access control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Determination of access authorization, authorization concept <input checked="" type="checkbox"/> Regulation for restoring data from backups <input checked="" type="checkbox"/> Regular verification of authorizations <input checked="" type="checkbox"/> Partial access options to databases and functions (read, write, execute) <input checked="" type="checkbox"/> Logging of file accesses and deletions at system level <p>Security systems (local virus scanner & firewall, SPAM filter in the mail system)</p> <p>Transfer control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Secure method of sending data between the Controller and third parties <input checked="" type="checkbox"/> Controlled destruction of data carriers (physical destruction or overwriting) <input checked="" type="checkbox"/> Controlled destruction of paper documents (sealed metal containers (so-called data protection garbage cans), disposal by service providers) <p>Input control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Differentiated user authorizations: Read/modify/delete <input checked="" type="checkbox"/> Organizational definition of input responsibilities <input checked="" type="checkbox"/> Logging of entries/deletions at system level <input checked="" type="checkbox"/> Log evaluation system <input checked="" type="checkbox"/> Obligation to maintain data secrecy | <p>Availability control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Data protection and backup concepts <input checked="" type="checkbox"/> Restrict access to server rooms to essential personnel only <input checked="" type="checkbox"/> Fire alarm systems/smoke detectors in server rooms <input checked="" type="checkbox"/> Waterless firefighting systems in separate rooms and fire compartment in the data center <input checked="" type="checkbox"/> Air-conditioned server rooms <input checked="" type="checkbox"/> CO2 fire extinguisher in the immediate vicinity of the server rooms <input checked="" type="checkbox"/> UPS system (uninterruptible power supply) <input checked="" type="checkbox"/> Power generator in the data center <p>Order control</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Contract design in accordance with legal requirements (Art. 28 GDPR) <input checked="" type="checkbox"/> Centralized recording of existing processors (uniform contract management) <input checked="" type="checkbox"/> External Processors and maintenance personnel, if not otherwise covered by a GCU, are given specific access that is only active during the intervention and deactivated the rest of the time. <p>Resilience and reliability check</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Dodge data centers <input checked="" type="checkbox"/> Data storage on RAID systems <input checked="" type="checkbox"/> Immediate and regular activation of available software and firmware updates <input checked="" type="checkbox"/> Periodic safety training and awareness campaigns within the organization. <input checked="" type="checkbox"/> Redundant power supply / UPS system / power generators / air conditioning / firefighting <input checked="" type="checkbox"/> Conducting penetration tests <p>Control procedure</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Internal procedure directories are updated at least once a year <input checked="" type="checkbox"/> Notification of new/changed data processing procedures to the data protection officer <input checked="" type="checkbox"/> Processes for reporting new/changed procedures are documented <p>Separation control</p> <p>Separation of customers (multi-client capability of the system used)</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Logical data separation (e.g. based on customer or client numbers) <p>Order-specific additional measures</p> <p>The aim is to minimize the particular risks that may arise from the specific order.</p> |
|--|---|

Asset Tracker

Attachment DPA for test package



A Vodafone Company

Appendix 2 Subprocessor

| Subprocessor, name, address | Commissioned services |
|---|--|
| Microsoft Ireland Operations Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland | Operation of a server infrastructure (Microsoft Azure Cloud) Zone "West Europe" |
| Vodafone GmbH Ferdinand-Braun-Platz 1 D-40549 Düsseldorf | Provision of connection services/connectivity Services according to the service description in the order form |
| Nordic Semiconductor ASA Otto Nielsens veg 12 7052 Trondheim, Norway | Cloud-based localization service for providing position data for Assisted-GPS (A-GPS), Single-Cell (SCCELL), Multi-Cell (MCELL) and Wi-Fi positioning. |
| Sentry.io Functional Software, Inc. 45 Fremont Street, 8th Floor San Francisco, CA 94105, USA | Error monitoring |