Supplementary Terms and Conditions for processing personal data on behalf of the Securitas Group

This Supplementary Contractual Terms and Conditions (EVB) apply to all orders placed by a Securitas company ("Principal" or "Responsible") to Business Partners ("Contractors" or "Processors") relating to processing of personal data. They supplement the respective General Terms and Conditions (GTC) of the German Securitas Group to Business Partners.

1. The subject matter and duration of data processing

The Contractor processes personal data on behalf of and under the direction of the Principal.

The object and duration of the data processing are specified in the respective assignment.

2. Specification of the data processing content

The scope, nature and purpose of the data collection, processing and/or use of personal data by the Contractor arise from the respective assignment.

The provision of contractually agreed data processing takes place exclusively in a Member State of the European Union. Any transfer to a third country requires the prior consent of the Principal and may only take place if the special conditions of Article 44 et seq. GDPR are met.

3. Categories of data, group of data subjects, nature of personal data

The category of data to be processed, the number of data subjects and the nature of the personal data are the result of the respective assignment.

4. Technical and organizational measures

(1) The Contractor shall document the implementation of the technical and organizational measures outlined in the run-up to the award of the contract before the start of the processing, in particular with regard to the actual execution of the contract, by self-declaration and hand it over to the Principal for examination (see example in **Annex 1** to this agreement). If accepted by the Principal, the documented measures become the basis of each assignment. Insofar as an audit of the Principal reveals a need for adaptation, the latter must be implemented by mutual agreement.

(2) The Contractor shall establish the safety in accordance with Articles 28 section 3 lit. c, 32 GDPR, in particular in conjunction with Article 5 section 1, section 2 GDPR. The measures to be taken are data security measures to ensure a level of protection in terms of the confidentiality, integrity, availability and resilience of the systems that is proportionate to the risk. The then current state of the art, the costs of implementation and the nature, scope and purpose of processing, as well as the different probability and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 section 1 GDPR must be taken into account [details in Annex 1].

(3) Technical and organizational measures shall be subject to technical progress and development. In this respect, the Contractor is permitted to implement alternative adequate measures. The level of safety of the measures laid down must not be lowered. Significant changes must be documented.

5. Correction, restriction and deletion of data

(1) The Contractor may not correct, delete or restrict the processing of the data processed on behalf of the Principal on its own initiative, but only in accordance with documented

instructions of the Principal. Insofar as a data subject addresses the Contractor directly in this regard, the Contractor shall immediately forward this request to the Principal.

(2) Insofar as within the scope of services the concept of deletion, the “right to be forgotten", correction, data portability and information according to documented instructions of the client must be observed directly by the Contractor.

6. Quality assurance and other obligations of the contractor

In addition to complying with the regulations of this order, the Contractor has legal obligations under Articles 28 to 33 GDPR; in particular, it ensures compliance with the following requirements:

a) Written appointment of a data protection officer to carry out his/her duties in accordance with Articles 38 and 39 GDPR. The contact details will be communicated to the Principal for the purpose of direct contact. A change of the data protection officer shall be communicated to the Principal without delay. If Contractor is not legally obliged to appoint a data protection office it will name Principal a data protection contact which, for the purpose of this document, shall be understood to be referred to as data protection officer as well.
b) Confidentiality in accordance with Articles 28 section 3 sentence2 lit. b, 29, 32 section 4 GDPR. The Contractor shall only use employees who have been obliged to maintain confidentiality and who have previously been familiarized with the provisions on data protection relevant to them in carrying out the work. The Contractor and any person under the authority of the Contractor who has access to personal data may process such data exclusively in accordance with the instructions of the Principal, including the powers conferred in this order, unless they are legally obliged to process them otherwise.
c) The implementation and compliance with all the technical and organizational measures required for this order in accordance with Articles 28 section 3 sentence 2 lit. c, 32 GDPR [details in Annex 1].
d) Principal and Contractor will cooperate with the supervisory authority if required.
e) Immediate information to the Principal on any audits and measures taken by the supervisory authority in so far as they relate to the order. This shall also apply to the extent that a supervisory authority investigates on the Contractor in the context of an administrative or criminal offence with regard to the processing of personal data.
f) Insofar as the Principal, for its part, is subject to an audit of the supervisory authority, an administrative offence or criminal proceedings, a liability claim of a data subject or a third party or any other claim in connection with the processing of personal data by the Contractor, the Contractor shall assist the Principal to the best of its ability.
g) The Contractor regularly monitors internal processes, as well as technical and organizational measures, to ensure that the processing is carried out in accordance with the requirements of applicable data protection law and that the protection of the rights of the data subject is ensured.
h) Verifiability of the technical and organizational measures taken against the client within the scope of its control powers in accordance with clause 8 of this EVB.

7. Subcontracting conditions

(1) Subcontracting relationships shall be those services which relate directly to the provision of the main service. This does not include ancillary services that the Contractor uses, for

example as telecommunication services, postal/transport services, maintenance and user services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. However, in order to ensure the data protection and data security of the customer's data, the Contractor is obliged to observe appropriate and legally compliant contractual agreements as well as control measures, even in the case of outsourced ancillary services.

(2) The Contractor may only commission subcontractors (other processors) with the prior, express, written or documented consent of the Principal. All contractual provisions in the contract chain must be forwarded to the further subcontractor.

(3) Further outsourcing by the subcontractor, in particular to third countries (outside the EU), is not permitted.

8. Control rights of the client

(1) Principal shall have the right to carry out audits or to have audits performed by expert auditors to be appointed on a case-by-case basis. Principal shall have the right to verify that the Contractor has complied with this EVB in the Contractor's business by means of random checks, which are normally to be notified in good time.

(2) Contractor shall ensure that Principal is able to verify compliance with the obligations of the Contractor under Article 28 GDPR. Contractor undertakes to provide Principal with the necessary information on request and, in particular, to prove the implementation of the technical and organisational measures.

(3) Proof of such measures, which do not only concern the specific contract, may be provided by:

a) compliance with approved codes of conduct in accordance with Article 40 GDPR
b) certification according to an approved certification procedure in accordance with Article 42 GDPR
c) current testates, reports or reports extracts from independent bodies (e.g. auditors, data protection officer, IT security department, data protection auditors, quality auditors)
d) appropriate certification by IT security or data protection audit (e.g. according to BSI basic protection)

9. Notification of breaches by the Contractor

(1) Contractor shall assist Principal in complying with the obligations relating to the security of personal data, reporting requirements in the event of data breaches, data protection impact assessments and prior consultations as set out in Articles 32 to 36 of the GDPR. These include

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing, as well as the predicted probability and severity of a possible breach of law by security vulnerabilities, and enable an immediate detection of relevant breach events
b) the obligation to report personal data breaches to Principal without delay

c) the obligation to assist Principal within the scope of its duty to provide information to the data subject and to provide him with all relevant information without delay
d) the Principal's support for its data protection impact assessment
e) the assistance of the Principal in the context of consultations with the supervisory authority

10. Authority of the Principal to issue instructions

(1) Principal confirms verbal instructions without delay (at least text form).

(2) Contractor shall inform Principal without delay if it considers that an instruction violates data protection regulations. Contractor is entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by Principal.

11. Deletion and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of Principal. This does not apply to backup copies to the extent necessary to ensure proper data processing and that is required to comply with legal retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by Principal – at the latest upon termination of the order – Contractor shall hand over to Principal all documents, processed and usage results drawn up and data relating to the contractual relationship or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The log of the deletion shall be submitted on request.

(3) Documentation intended to prove the order and proper processing of data shall be kept by the Contractor in accordance with the respective retention periods beyond the end of the order. It may hand them over to Principal at the end of the order for its discharge.

Annex 1
Declaration
of compliance with technical organizational measures in the processing of personal data

Insofar as the processing of personal data within the meaning of Article 28 GDPR is part of the services I provide on behalf of or for Securitas, this is carried out in accordance with the Supplementary Terms and Conditions (EVB) for processing personal data on behalf of the Securitas Group. I can view and download them at any time under www.securitas.de/subunternehmer.

The category and type of data to be processed shall be communicated by Securitas as part of the order.

In the processing, I guarantee an adequate level of protection within the meaning of Article 32 GDPR by appropriate technical and organizational measures. I attach these as an annex to this Declaration as proof.

I will inform Securitas immediately about any changes in personnel engaged with processing of personal data (e.g. due to termination of employment) along with the information for which data the personnel was responsible.

Our data protection officer or data protection contact is:

Name:

Business address:

Phone: E-mail:

I confirm the above information provided in this statement is correct.

This Declaration becomes part of all legal relations that I or the company I represent enters into with companies of the Securitas Group.

Name of Business Partner: _____

Name of Authorized Signatory: _____

Location/date: _____

_____ _____

Signature Company Stamp

Annex TOM to the Declaration
on compliance with technical organizational measures in the processing of data

General measures	Yes	No	General measures	Yes	No
Internal policies for data protection and IT security, including practices under applicable legislation, are defined, implemented, regularly reviewed and updated.			Authorization control for system access of personnel and third parties (e.g. service providers, self-employed, consultants, developers) taking into account the sensitivity and criticality of data processing is implemented and limited to the absolutely necessary minimum (need-to-know principle). A process for managing system access (application, approval, withdrawal, ...) is also implemented.		
Responsibilities for data protection and data security are defined (e.g. IT security officer, data protection officer (if legally required))			Access to systems (computers, devices) requires authentication via individual and password-protected user accounts (password requirements are set according to the current state of the art)		
Employees who process personal data are obliged to maintain confidentiality			After repeated incorrect access attempts or automatically when a user is inactive for a certain period of time, access to IT systems is blocked and a new login is required		
Employees are regularly (at least annually) trained on data protection and data security			IT systems in which personal data are processed are protected by measures according to the current state of the art against unauthorized access from other networks (e.g. firewalls, virus scanners).		
Conduct regular internal audits to ensure compliance with data protection and information security policies and to review the adequacy and effectiveness of policies chosen			A data backup concept is defined and implemented		
Special categories of personal data are only stored encrypted			An operational continuity strategy, including recovery times, is implemented		
Encryption when processing personal data when transferring personal data online or through mobile media (e.g. notebooks, laptops, hard drives, CDs, DVDs, USB-sticks, cassettes, floppy disks, memory cards, etc.)			Retention periods for personal data set by the controller may be implemented.		
Procedures/guidelines for an appropriate separation of data sets (e.g. separation of data from different managers, separation of test/development data and production data)			Standardized, documented and verified contracts of used sub-processors processing personal data are available If other processors are employed by the processor (sub-processors) contracts are concluded, documented and verified in accordance with the applicable regulations.		
Authorization control for the physical access of personnel and third parties (visitors, customers, cleaning staff, manual workers, etc.) to facilities and rooms (taking into account the sensitivity and criticality of data processing) and a process for access management (application, approval, withdrawal, ...) are implemented					

Name Business Partner:

Signature Business Partner:

Annex TOM to the Declaration
on compliance with technical organizational measures in the processing of data

Organizational measures	Yes	No	Organizational measures	Yes	No
IT guidelines according to known frameworks (e.g. ISO 27001, ISO 27018 (for cloud-based services), BS 10012 or equivalent standards)			Provide further internal controls in accordance with ISAE 3402 Type II / SOC 2 Type 2 or other applicable frameworks		
Sub-processors that process personal data are regularly reviewed.			Public concepts and/or procedures for the controlled destruction of physical storage media in the processing of personal data (e.g. after the expiry of the retention period or on request from the controller)		
Clear distinction between the responsibilities of the processor and the person in charge					

Physical access control measures	Yes	No	Physical access control measures	Yes	No
ID cards or access cards			biometric ID cards		
Safety or electronic locks			Key		
Identification of persons who need access to the facilities			Visitor passes for third parties		
Logging of access to facilities			Security alarm systems or other appropriate security measures		
Construction measures (fences, video surveillance, closed doors, gates and windows, etc.)			Separate security areas with their own access management ("closed shops")		

IT Infrastructure and Software	Yes	No	IT Infrastructure and Software	Yes	No
Guidelines for documentation of software and IT procedures			Documentation of the IT infrastructure, including system interfaces		
Centralized purchasing of hardware and software			Approval procedures for hardware, software and IT technology		
Data protection and IT security requirements are addressed as part of software release management processes			Software used is kept up-to-date (e.g. updates, patches, fixes, etc.)		
Execution of risk and vulnerability analysis			Lines and processes for remote maintenance and/or system maintenance		

Data management	Yes	No	Data management	Yes	No
Documentation which persons are authorized to enter personal data into data processing systems			Protection for data entry, read, block, and deletion of personal data		
Special categories of personal data are pseudonymized, unless required in plain text			Securing data areas in which personal data is (temporarily) created		
Separation of pseudonymized personal data from the original data			Identification of internal and external data		

Name Business Partner:

Signature Business Partner:

Annex TOM to the Declaration
on compliance with technical organizational measures in the processing of data

Logging of access to personal data (in particular use, modification and deletion of data, by whom and with time stamps)			Personal data used for different purposes and customers is stored separately (physical separation)		
The network is segmented so that at least the front-end system is disconnected from the back-end systems					
IT System Controls	**Yes**	**No**	**IT System Controls**	**Yes**	**No**
Systems are automatically locked if a user is inactive for an extended period of time.			Logging of all processes (e.g. audit trails and access attempts)		
Back-end systems are hardened to prevent attackers from gaining unauthorized access					

Operational continuity measures	**Yes**	**No**	**Operational continuity measures**	**Yes**	**No**
An emergency plan for critical systems, including clear steps and procedures regarding potential hazards, activation triggers, activation decision-making process, recovery steps and time			Log the activation and execution of an emergency plan, including decisions taken, actions taken, and final recovery time		
Servers are set up in a separately secured server room or data center			Data backups are stored fire- and water-protected		
Emergency generators and/or uninterruptible power supply are available			Emergency exercises are regularly carried out		
Backups are made at regular intervals			Backups are kept in a secure location outside the IT department		
Mirroring			The serviceability of the backups is regularly checked		
Alternative storage locations for emergency backups are available					

Transmission controls	**Yes**	**No**	**Transmission controls**	**Yes**	**No**
Data carriers are only issued to authorized persons or (external) parties			Use of external storage media (especially USB-sticks, external hard drives, SD cards, CD and DVD burners) is limited by technical measures (e.g. software for interface controllers or complete deactivation of interfaces)		
Software in which transmission to third parties cannot be excluded is not used for transmission to Securitas (e.g. Skype, Google Chrome, Google Desktop, Google Toolbar, translation software, social media tools, etc.)			Documentation of remote areas/destinations to which a transmission is planned and the transmission path (logical path)		
Full, proper and secure data transfer			Courier services, personal collection, proof at the end of the transport		
Implementation of filtering measures (URL filters, attachment filters for e-mail, etc.)					

Name Business Partner:

Signature Business Partner: