Securitas

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/geschaeftspartner.

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

Appendix TOM to the Declaration
of compliance with technical organizational measures in the processing of personal 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.		

Name Business Partner:

Signature Business Partner:

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

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					

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					

Name Business Partner:

Signature Business Partner:

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

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		

Name Business Partner:

Signature Business Partner:

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

Separation of pseudonymized personal data from the original data			Identification of internal and external 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		

Name Business Partner:

Signature Business Partner:

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: