Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von personenbezogenen Daten

Sofern die Verarbeitung von personenbezogenen Daten im Sinne des Art. 28 DSGVO Bestandteil der Leistungen ist, die ich im Auftrag von Securitas erbringe, erfolgt diese gemäß den Ergänzenden Vertragsbedingungen (EVB) für die Auftragsverarbeitung im Auftrag der Securitas Gruppe. Diese kann ich jederzeit unter www.securitas.de/subunternehmer einsehen und abrufen.

Die Kategorie und Art der zu verarbeitenden Daten teilt Securitas im Rahmen der Bestellung mit.

Bei der Verarbeitung gewährleiste ich ein angemessenes Schutzniveau im Sinne des Art. 32 DSGVO durch geeignete technische und organisatorische Maßnahmen. Diese füge ich als Anhang zu dieser Eigenerklärung als Nachweis bei.

Ich informiere Securitas unverzüglich über jede Veränderung in dem mit der Verarbeitung beschäftigten Mitarbeiterstamm (z.B. Ende des Arbeitnehmerverhältnisses) und die durch die jeweilige Person verarbeiteten Daten.

Als Datenschutzbeauftragten bzw. Datenschutzansprechpartner habe ich benannt:

Name:

Geschäftsanschrift:

Telefon: E-Mail:

Ich bestätige die Richtigkeit der in dieser Erklärung getätigten Angaben.

Diese Erklärung wird Bestandteil sämtlicher Rechtsbeziehungen die ich bzw. die von mir vertretene Gesellschaft zu Unternehmen der Securitas Gruppe unterhalte.

Name des Geschäftspartners: _____

Name d. Unterzeichners: _____

Ort/Datum: _____

_____ _____

Unterschrift Firmenstempel

Anhang TOM zur Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von personenbezogenen Daten

Allgemeine Maßnahmen	**Ja**	**Nein**	**Allgemeine Maßnahmen**	**Ja**	**Nein**
Interne Richtlinien für Datenschutz und IT-Sicherheit, einschließlich von Vorgehensweisen gemäß anwendbaren Rechtsvorschriften, sind definiert, umgesetzt, werden regelmäßig überprüft und auf den neuesten Stand gebracht.			Autorisierungskontrolle für den Systemzugang von Personal und Dritten (z.B. Dienstleister, Selbstständige, Berater, Entwickler) unter Berücksichtigung der Sensibilität und Kritikalität der Datenverarbeitung ist implementiert und auf das absolut notwendige Mindestmaß begrenzt (need-to-know Prinzip). Ein Prozess für die Verwaltung des Systemzugangs (Beantragung, Genehmigung, Entzug, …) ist ebenfalls implementiert.		
Verantwortlichkeiten für Datenschutz und Datensicherheit sind definiert (z.B. IT Sicherheitsbeauftragte/r, Datenschutzbeauftragte/r (falls rechtlich erforderlich))			Der Zugang zu Systemen (Computern, Geräten) erfordert eine Authentisierung über individuelle und passwortgeschützte Benutzerkonten (Passwortanforderungen sind gemäß dem aktuellen Stand der Technik festgelegt)		
Mitarbeiter, welche personenbezogene Daten verarbeiten, sind zur Geheimhaltung verpflichtet			Nach wiederholten falschen Zugangsversuchen oder automatisch, wenn ein Anwender über einen bestimmten Zeitraum inaktiv ist, wird der Zugang zu IT-Systemen gesperrt, woraufhin ein neues Einloggen erforderlich ist		
Mitarbeiter werden regelmäßig (mindestens jährlich) zum Datenschutz und zu Datensicherheit geschult			IT-Systeme, in denen personenbezogene Daten verarbeitet werden, werden durch Maßnahmen gemäß dem aktuellen Stand der Technik vor unautorisiertem Zugang von anderen Netzwerken geschützt (z. B. Firewalls, Virusscanner).		
Durchführung regelmäßiger interner Audits, um die Einhaltung von Richtlinien zum Datenschutz und zur Informationssicherheit sicherzustellen und Überprüfung hinsichtlich der Angemessenheit und Wirksamkeit gewählter Maßnahmen			Ein Datensicherungskonzept ist festgelegt und implementiert		
Besondere Kategorien personenbezogener Daten werden nur verschlüsselt gespeichert			Eine Betriebskontinuitätsstrategie, einschließlich der Wiederherstellungszeiten, ist implementiert		
Verschlüsselung bei der Verarbeitung personenbezogener Daten bei online Übertragung oder durch mobile Medien (z.B.			Vom Verantwortlichen festgelegte Aufbewahrungsfristen für personenbezogene Daten können umgesetzt werden.		

Name Geschäftspartner:

Unterschrift Geschäftspartner:

Notebooks, Laptops, Festplatten, CDs, DVDs, USB-Sticks, Kassetten, Disketten, Speicherkarten, usw.)					
Verfahren/ Richtlinien für eine angemessene Trennung von Datensätzen (z.B. Trennung von Daten unterschiedlicher Verantwortlicher, Trennung von Test/ Entwicklungsdaten und Produktivdaten)			Standardisierte, dokumentiere und überprüfte Verträge von verwendeten Unterauftragsverarbeitern, die personenbezogene Daten verarbeiten, sind vorhanden Sofern vom Auftragsverarbeiter weitere Verarbeiter eingesetzt werden (Sub-Auftragsverarbeiter) werden gemäß der geltenden Vorschriften Verträge geschlossen, dokumentiert und überprüft.		
Autorisierungskontrolle für den physischen Zutritt von Personal und Dritten (Besucher, Kunden, Putzpersonal, Handarbeiter, usw.) zu Einrichtungen und Räumen (unter Berücksichtigung der Sensibilität und Kritikalität der Datenverarbeitung) und ein Prozess für die Zugangsverwaltung (Beantragung, Genehmigung, Entzug, ...) sind implementiert					

Organisatorische Maßnahmen	**Ja**	**Nein**	**Organisatorische Maßnahmen**	**Ja**	**Nein**
IT Richtlinien gemäß bekannter Frameworks (z.B. ISO 27001, ISO 27018 (für Cloud-basierte Serviceleistungen), BS 10012 oder äquivalente Standards)			Bereitstellung von weiteren internen Kontrollen gemäß ISAE 3402 Type II- / SOC 2 Type 2 oder anderen anwendbaren Frameworks		
Sub-Auftragsverarbeiter, die personenbezogene Daten verarbeiten, werden regelmäßig überprüft.			Löschkonzepte und/ oder Vorgehensweisen für die kontrollierte Vernichtung physischer Speichermedien bei der Verarbeitung personenbezogener Daten (z.B. nach Ablauf der Aufbewahrungsfrist oder auf Anfrage vom Verantwortlichen)		
Klare Abgrenzung zwischen den Verantwortungsbereichen des Auftragsverarbeiters und des Verantwortlichen					

Name Geschäftspartner:

Unterschrift Geschäftspartner:

Anhang TOM zur Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von personenbezogenen Daten

Physische Zugangskontrollmaßnahmen	**Ja**	**Nein**	**Physische Zugangskontrollmaßnahmen**	**Ja**	**Nein**
Ausweise oder Zutrittskarten			biometrische Ausweise		
Sicherheits- oder elektronische Schlösser			Schlüssel		
Identifikation von Personen, die Zutritt zu den Einrichtungen benötigen			Besucherausweise für Dritte		
Protokollierung des Zutritts in Einrichtungen			Sicherheitsalarmsysteme oder andere angemessene Sicherheitsmaßnahmen		
Bauliche Maßnahmen (Zäune, Videoüberwachung, geschlossene Türen, Tore und Fenster, etc.)			Gesonderte Sicherheitsbereiche mit eigener Zutrittsverwaltung (“closed shops”)		

IT Infrastruktur und Software	**Ja**	**Nein**	**IT Infrastruktur und Software**	**Ja**	**Nein**
Richtlinien für die Dokumentation von Software und IT Verfahren			Dokumentation der IT Infrastruktur, einschließlich der Systemschnittstellen		
Zentralisierter Einkauf von Hardware und Software			Freigabeverfahren für Hardware, Software und IT Technik		
Datenschutz- und IT Sicherheitsanforderungen werden im Rahmen von Softwarerelease Managementprozessen behandelt			Verwendete Software wird auf dem aktuellsten Stand gehalten (z.B. durch Updates, Patches, fixes, etc.)		
Durchführung von Risiko und Schwachstellenanalyse			Richtlinien und Prozesse für Remote-Wartungsmaßnahmen und/ oder Systembetreuung		

Datenmanagement	**Ja**	**Nein**	**Datenmanagement**	**Ja**	**Nein**
Es wird dokumentiert, welche Personen autorisiert sind, personenbezogene Daten in Datenverarbeitungssystemen einzugeben			Schutzmaßnahmen für Dateneingabe, für das Lesen, Blockieren und Löschen von personenbezogenen Daten		
Besondere Kategorien personenbezogener Daten werden, sofern nicht im Klartext benötigt, pseudonymisiert			Sicherung von Datenbereichen in denen personenbezogene Daten (temporär) angelegt werden		

Name Geschäftspartner:

Unterschrift Geschäftspartner:

Anhang TOM zur Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von personenbezogenen Daten

Trennung von pseudonymisierten personenbezogenen Daten von den ursprünglichen Daten			Kennzeichnung von internen und externen Daten		
Protokollierung von Zugriffen auf personenbezogene Daten (insbesondere Benutzung, Modifizierung und Löschung von Daten, von wem und mit Zeitstempel)			Personenbezogene Daten, die für verschiedene Zwecke und Kunden verwendet werden, werden separat gespeichert (physische Trennung)		
Das Netzwerk ist segmentiert, sodass zumindest das Front-End-System von den Back-End-Systemen getrennt ist					
IT Systemkontrollen	**Ja**	**Nein**	**IT Systemkontrollen**	**Ja**	**Nein**
Systeme werden automatisch gesperrt, wenn ein Anwender über einen längeren Zeitraum inaktiv ist			Protokollierung aller Abläufe (z.B. Audit Trails und Zugriffsversuche)		
Back-End-Systeme sind gehärtet um zu verhindern, dass sich Angreifer unautorisierten Zugang verschaffen können					

Betriebliche Kontinuitätsmaßnahmen	**Ja**	**Nein**	**Betriebliche Kontinuitätsmaßnahmen**	**Ja**	**Nein**
Ein Notfallplan für kritische Systeme, einschließlich klaren Schritten und Verfahren hinsichtlich möglicher Gefahren, Auslöser für die Aktivierung, Entscheidungsprozess für eine Aktivierung, Wiederherstellungsschritte und -zeit			Protokollierung der Aktivierung und Ausführung eines Notfallplans, einschließlich der getroffenen Entscheidungen, getroffenen Maßnahmen und der endgültigen Wiederherstellungszeit		
Server sind in einem separat gesicherten Serverraum oder Datencenter aufgebaut			Datensicherungen werden brand- und wassergeschützt aufbewahrt		
Notfallgeneratoren und/ oder unterbrechungsfreie Stromversorgung sind vorhanden			Regelmäßig werden Notfallübungen durchgeführt		
Sicherungskopien werden in regelmäßigen Abständen erstellt			Sicherungskopien werden außerhalb der IT Abteilung an einem sicheren Ort aufbewahrt		
Datenspiegelung			Die Instandsetzbarkeit der Sicherungskopien wird regelmäßig überprüft		
Alternative Aufbewahrungsorte für Sicherungskopien für Notfälle sind vorhanden					

Name Geschäftspartner:

Unterschrift Geschäftspartner:

Anhang TOM zur Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von personenbezogenen Daten

Übermittlungskontrollen	**Ja**	**Nein**	**Übermittlungskontrollen**	**Ja**	**Nein**
Datenträger werden nur an autorisierte Personen oder (externe) Parteien herausgegeben			Benutzung externer Speichermedien (insbesondere USB-Sticks, externe Festplatten, SD Karten, CD und DVD Brenner) wird durch technische Maßnahmen begrenzt (z.B. Software für Schnittstellenkontroller oder komplette Deaktivierung von Schnittstellen)		
Software, bei der die Übertragung an Dritte nicht ausgeschlossen werden kann, wird zur Übertragung an Securitas nicht verwendet (z.B. Skype, Google Chrome, Google Desktop, Google Toolbar, Übersetzungssoftware, Social Media Tools, usw.)			Dokumentierung von remote Bereichen/ Bestimmungsorten zu welchen eine Übertragung vorgesehen ist und der Übertragungsweg (logischer Pfad)		
Vollständige, ordnungsgemäße und gesicherte Datenübertragung			Kurierdienstleistungen, persönliche Abholung, Nachweis bei Abschluss des Transports		
Implementierung von Filtermaßnahmen (URL Filter, Filter bei E-Mail anhängen, usw.)					

Name Geschäftspartner:

Unterschrift Geschäftspartner: