Ergänzende Vertragsbedingungen für die Auftragsverarbeitung im Auftrag der Securitas Gruppe

Diese Ergänzenden Vertragsbedingungen (EVB) gelten für alle Aufträge einer Securitas Gesellschaft („Auftraggeber“ bzw. „Verantwortlicher“) gegenüber Geschäftspartnern („Auftragnehmer“ bzw. „Auftragsverarbeiter“), die eine Auftragsverarbeitung zum Gegenstand haben. Sie ergänzen die jeweiligen Allgemeinen Geschäftsbedingungen (AGB) der deutschen Securitas Gruppe gegenüber Geschäftspartnern.

1. Gegenstand und Dauer des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Gegenstand sowie Dauer der Datenverarbeitung werden in der jeweiligen Beauftragung konkretisiert.

2. Konkretisierung des Auftragsinhalts

Umfang, Art und Zweck der Datenerhebung, -verarbeitung und/oder –nutzung personenbezogener Daten durch den Auftragnehmer ergeben sich aus der jeweiligen Beauftragung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Datenkategorien, Kreis der betroffenen Personen, Art der personenbezogenen Daten

Die Kategorie der zu verarbeitenden Daten, der Kreis der betroffenen Personen, sowie die Art der personenbezogenen Daten ergeben sich aus der jeweiligen Beauftragung.

4. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung per Eigenerklärung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Muster in **Anlage 1** zu dieser Vereinbarung). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage ein jeder Beauftragung. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet,

alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf „Vergessen werden", Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Im Falle, dass der AN keinen Datenschutzbeauftragten zu benennen hat, ist dem AG ein Datenschutzansprechpartner zu benennen, welcher zum Zwecke dieser Vereinbarung ebenfalls unter dem Begriff „Datenschutzbeauftragter" zu verstehen ist.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf das Datengeheimnis verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in der Eigenerklärung nach Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieser EVB.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger, ausdrücklicher, schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(3) Eine weitere Auslagerung durch den Unterauftragnehmer, insbesondere in Drittstaaten, ist nicht gestattet.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

10. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger

Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage 1
Eigenerklärung
über die Einhaltung technisch organisatorischer Maßnahmen bei der Verarbeitung von Daten

Sofern die Verarbeitung von Daten im Sinne des Art. 28 DSGVO Bestandteil der Leistungen ist, die ich im Auftrag von Securitas erbringe, erfolgt diese gemäß den Allgemeinen Bedingungen für 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 die in der Anhang TOM bezeichneten technischen und organisatorische Maßnahmen.

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 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 (z.B. über Arbeitsvertrag, separate Geheimhaltungsvereinbarung, sonstige berufliche Verpflichtungen)			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 verarbeitet			Eine Betriebskontinuitätsstrategie, einschließlich der Wiederherstellungszeiten, ist implementiert		
Verschlüsselung bei der Verarbeitung personenbezogener Daten bei online Übertragung oder durch mobile Medien (z.B. Notebooks, Laptops, Festplatten, CDs, DVDs, USB sticks, Kassetten, Disketten, Speicherkarten, usw.)			Vom Verantwortlichen festgelegte Aufbewahrungsfristen für personenbezogene Daten können umgesetzt werden.		
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					

Name Geschäftspartner:

Unterschrift Geschäftspartner:

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

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					

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 pseudonymisiert			Sicherung von Datenbereichen in denen personenbezogene Daten (temporär) angelegt werden		
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)		

Name Geschäftspartner:

Unterschrift Geschäftspartner:

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

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					

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 abgeschaltet (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: