

Checkliste Auftragnehmer-Kontrolle zur Auftragsverarbeitung

Auftragsverarbeiter (Auftragnehmer, AN)	Datum	Name	Unterschrift

Diese Checkliste dient der Dokumentation der Umsetzung der Vorgaben des Artikel 28 in Verbindung mit Artikel 32 der Datenschutz-Grundverordnung (DSGVO). Die Checkliste ist durch den Auftragsverarbeiter auszufüllen und zu unterzeichnen. Bitte achten Sie auf den Hinweis MUSS oder KANN Anforderung in Spalte A.

Checkliste Auftragnehmer-Kontrolle zur Auftragsverarbeitung

Typ der Anforderung	Vorgabe	erfüllt	nicht erfüllt	Hinweise des AG	Bemerkungen vom AN
Datenschutz-Management					
MUSS	Der AN hat einen verantwortliche Ansprechpartner zur Klärung aller fachlichen, technischen und organisatorischen Fragen.				Name: Kontaktdaten:
MUSS	Der AN hat eine*n Datenschutzbeauftragte*n (DSB) bestellt bzw. eine*n Ansprechpartner*in für Datenschutz benannt.			Nur falls der AN zu einer Benennung eines DSB gesetzlich verpflichtet ist, MUSS hier ein DSB genannt werden. Ansonsten MUSS ein Ansprechpartner für Datenschutz eingetragen werden.	Name: Kontaktdaten:
MUSS	Arbeits-/ Verfahrensanweisungen zur IT-Sicherheit sind beim AN vorhanden.			-	
MUSS	Arbeits-/ Verfahrensanweisungen zum Datenschutz sind beim AN vorhanden.			-	
MUSS	Der AN verpflichtet seine Mitarbeiter auf Vertraulichkeit (Art. 28 (3b) DSGVO).			-	
MUSS	Der DSB der AN kontrolliert den AN bezüglich der Einhaltung von Datenschutzvorgaben.			-	
MUSS	Ein Verfahrensverzeichnis gem. Art. 30 (2) DSGVO ist beim AN vorhanden.			-	
MUSS	Die Beschäftigten des AN werden regelmäßig zum Thema Datenschutz geschult.			-	
KANN	Der AN erlaubt mobiles Arbeiten zur Auftragserfüllung.			-	
Bitte folgende Zeile nur ausfüllen, wenn AN mobiles Arbeiten erlaubt:					
MUSS	Arbeits-/ Verfahrensanweisungen zum mobilen Arbeiten sind vorhanden.			-	
Auftragskontrolle					
MUSS	Der AN sichert durch geeignete Maßnahmen zu, dass personenbezogene Daten zur Auftragserfüllung ausschließlich nach Weisungen des AG verarbeitet werden.			-	
MUSS	Die Datenverarbeitung beim AN von personenbezogenen Daten zur Auftragserfüllung erfolgt ausschließlich innerhalb der EU/EWR.			Erläuterung: Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in einem Drittland, für das ein angemessenes Schutzniveau gemäß Art. 45 DSGVO festgestellt wurde, statt.	
Bitte folgende zwei Zeilen nur ausfüllen, wenn Unterauftragnehmer eingesetzt werden (gemäß Vereinbarung zur Auftragsverarbeitung, Anhang B):					
MUSS	Die Datenverarbeitung beim Unterauftragnehmer erfolgt nur auf Basis eines Vertrages oder eines Rechtsinstruments gemäß Art. 28 Abs. 3 DSGVO.			-	
MUSS	Die Datenverarbeitung beim Unterauftragnehmer von personenbezogenen Daten zur Auftragserfüllung erfolgt ausschließlich innerhalb der EU/EWR.			Erläuterung: Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Drittland, für das ein angemessenes Schutzniveau gemäß Art. 45 DSGVO festgestellt wurde, statt.	
Zutrittskontrolle					
MUSS	Der AN sichert zu, durch geeignete Maßnahmen Unbefugten den (physische) Zutritt zu Büro-Räumlichkeiten des AN, in den personenbezogene Daten des AG verarbeitet werden, zu verwehren. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs (technische und organisatorische Maßnahmen) des AN zu verweisen.			z.B. mechanisch oder elektronisch gesichertes Zutrittsystem, Pforte, Werkschutz	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Der AN sichert zu, durch geeignete Maßnahmen Unbefugten den (physische) Zutritt zu Server-Räumlichkeiten des AN, in den personenbezogene Daten des AG verarbeitet werden, zu verwehren. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			z.B. Werkschutz, separate Zutrittskontrolle im Vergleich zu den Büroräume, Alarmanlage, Videoanlage zu den Serverräumen zählen hier auch zentrale Datenknoten / Übergang zum Internet.	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Der AN sichert zu, durch geeignete Maßnahmen den (physische) Zutritt von Besuchern zu Räumlichkeiten des AN, in den personenbezogene Daten des AG verarbeitet werden, zu regeln. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			z.B. Trennung von Bearbeitungs- und Publikumszonen, Besucherregelungen, Dokumentation von Besuchern	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
Zugangskontrolle					
MUSS	Der AN sichert zu, durch geeignete Maßnahmen Unbefugten der Zugang zu IT-Systemen des AN, in den personenbezogene Daten des AG verarbeitet werden, zu verwehren. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			Für den Fall, dass die Datenverarbeitung der personenbezogenen Daten der Stromnetz Berlin GmbH durch den AN ausschließlich in Systemen des AG erfolgt, bezieht sich die Frage nur auf den Zugang auf Clients in der Verantwortung des AN. z.B. (automatische) Bildschirmsperre bei Pausen mit Passwort-Aktivierung	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Passwörter für IT-Systeme entsprechen den Vorgaben des IT-Grundschutz-Kompodium des BSI oder es gibt vergleichbare Regelungen.			z.B. bezüglich Passwort-Komplexität Wenn "vergleichbare Regelungen" realisiert wird, sind diese Regelung zu beschreiben	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Nutzerkonten und Administratorkonten sind voneinander getrennt.			-	
MUSS	Es gibt keine „Gruppen-Passwörter“.			-	

Checkliste Auftragnehmer-Kontrolle zur Auftragsverarbeitung

Typ der Anforderung	Vorgabe	erfüllt	nicht erfüllt	Hinweise des AG	Bemerkungen vom AN
Zugriffskontrolle					
MUSS	Der AN sichert zu, durch geeignete Maßnahmen den Zugriff in IT-Systemen des AN für Befugte auf die Daten und Berechtigungen, die für ihre Aufgaben notwendig sind, einzuschränken. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			Die Frage bezieht sich ausschließlich auf den Zugriff auf personenbezogene Daten in der Verantwortung der Stromnetz Berlin GmbH.	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Es gibt ein Berechtigungskonzept für jedes IT-System, welches personenbezogenen Daten des AG verarbeitet.			-	
MUSS	Es gibt ein definiertes Verfahren für die Vergabe von administrativen Zugriffsrechten.			-	
Datenträgerkontrolle					
MUSS	Der AN sichert durch geeignete Maßnahmen eine geschützte Speicherung von digitalen personenbezogenen Daten zu. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			Bezieht sich auf IT-Systeme, Dateien etc. z.B. verschlüsselte Clients	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden. dabei Maßnahmen für mobile Clients (z.B. Laptops für Außendienstmitarbeiter) berücksichtigen
MUSS	Der AN sichert zu, durch geeignete Maßnahmen eine geschützte Aufbewahrung von Papierdokumenten u.ä. mit personenbezogenen Daten sicher zustellen. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			Bezieht sich auf Papierdokumente etc. mit personenbezogenen Daten in der Verantwortung der Stromnetz Berlin GmbH.	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Der AN sichert zu, Papierdokumente bzw. Datenträger mit personenbezogenen Daten des AG fachgerecht zu entsorgen.			-	
MUSS	Arbeits-/ Verfahrensanweisungen zur Entsorgung von Papierdokumenten bzw. Datenträgern sind vorhanden.			-	
Trennbarkeit					
MUSS	Der AN sichert zu, dass die Daten des AG durch den AN physisch/logisch von Daten anderer Firmen getrennt verarbeitet werden.			z.B. durch Mandantentrennung	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
Eingabekontrolle					
MUSS	Der AN sichert zu, geeignete Maßnahmen zur Überwachung der Datenverarbeitung und Identifikation von Sicherheitsrisiken zu betreiben. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			-	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
Transportkontrolle					
MUSS	Der AN sichert zu, dass jeder Transport von personenbezogenen Daten auf digitalen bzw. physischem Weg derart geschützt erfolgt, dass ein unbefugter Zugriff, eine Kopie, eine Veränderung oder eine Löschung verhindert wird. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			z. B: Sensible Daten (z. B. _____) dürfen nicht in "normalen" E-Mails ausgetauscht werden. Wenn eine Übertragung von solchen Daten per E-Mail erfolgen soll, so muss diese Ende-zu-Ende verschlüsselt sein.	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	E-Mails zwischen AG und AN sind Ende-zu-Ende verschlüsselt.			-	
Wiederherstellbarkeit					
MUSS	Der AN sichert zu, dass die eingesetzten IT-Systeme im Störfall wiederhergestellt werden können. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			-	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Es gibt für Server ein regelmäßiges Backup (Datensicherung).			-	
MUSS	Die Aufbewahrung von Sicherungsdатenträgern erfolgt räumlich getrennt von den Produktivsystemen.			-	
Verfügbarkeitskontrolle					
MUSS	Der AN sichert zu, dass personenbezogene Daten des AG bei Bedarf verfügbar sind und gegen Zerstörung oder Verlust geschützt sind. Die konkreten Maßnahmen sind zu beschreiben bzw. es ist auf das entsprechende Kapitel in den TOMs des AN zu verweisen.			-	Bitte hier die Beschreibung ihrer Maßnahmen einfügen. Ein Verweis auf ein entsprechendes Kapitel der TOMs des Auftragnehmers ist in gleicher Weise möglich, dann müssen die TOMs ebenfalls Vertragsbestandteil werden.
MUSS	Es gibt ein Brandschutzkonzept für alle Räumlichkeiten des AN, in denen personenbezogene Daten des AG verarbeitet werden.			-	
MUSS	Es gibt einen Notfallplan beim AN (Wiederanlaufplan).			-	