



Verarbeitungsverzeichnis für Auftragsverarbeiter

Um Ihren geschätzten Auftrag zu Verarbeiten erlaube ich mir folgende Daten zu erheben und zu speichern

Datenverarbeitungsverzeichnis nach Art 30 Abs 2 EU-Datenschutz-Grundverordnung (DSGVO)

Stammdaten des Auftragsverarbeiters	Name und Kontaktdaten des Auftragsverarbeiters/der Auftragsverarbeiter 1) Name und Anschrift: 2) E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.): 3) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten des Auftragsverarbeiters ¹ :
Stammdaten zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung	Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen (=Auftraggeber) 1) Name(n) und Anschrift(en): 2) E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.): 3) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Datenschutzbeauftragten:1 4) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des Vertreters des (der) Verantwortlichen ² :

¹ Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. Hinweis: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „Datenschutzbeauftragter“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (z.B. „Datenschutzkoordinator“). Dieser kann, muss aber nicht ins Verzeichnisse aufgenommen werden..

² Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.



Kategorien von Verarbeitungen	<p>Kategorien von Verarbeitungen, die im Auftrag des konkreten Verantwortlichen durchgeführt werden (Angabe der angebotenen Leistung, die im Zusammenhang mit der Verarbeitung personenbezogener Daten steht)</p> <p>Optional:</p> <ul style="list-style-type: none">• Art. 28 Abs. 3 - Weisungen des Auftraggebers
Auftragsdatenverarbeitung <i>Alles Rund um Ihren Auftrag/ Druckabwicklung oder Softwareinstallationen</i>	<p>Angabe der angebotenen Leistung, die im Zusammenhang mit der Verarbeitung personenbezogener Daten steht:</p> <ul style="list-style-type: none">• Lösungsverfahren im Allgemeinen - Sie haben jederzeit das Recht auf Löschung Ihrer Daten• Mitwirkungspflicht bei Betroffenenrechten im Zuge des Auftragsverhältnisses• Art. 28 Abs. 2 - Sub-Auftragsverhältnisse In erster Linie sind Druckereien und Lieferanten gemeint, die Ihren Auftrag produzieren/ weiterverarbeiten und zustellen
Übermittlung Drittstaaten	<p>Übermittlung von personenbezogenen Daten in Drittländer, inkl. internationale Organisationen</p> <p><i>Ggf. Onlinedruckereien im EU Raum, Hosting und oder Plugin Dienstleister für Ihre Webseite (international)</i></p> <ol style="list-style-type: none">1) Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Binding Corporate Rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)



Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen	<ol style="list-style-type: none">1) Vertraulichkeitⁱ:2) Integritätⁱⁱ:3) Verfügbarkeit und Belastbarkeitⁱⁱⁱ:4) Pseudonymisierung und Verschlüsselung:5) Evaluierungsmaßnahmen^{iv}:
--	--

Herzlichen Dank!
MfG
Nina Stadelmann

Hinweise

Dieses Musterverzeichnis wurde mit größter Sorgfalt erstellt und kann laufend aktualisiert werden. Für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters sowie auch für weiterführende Links können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster bereitgestellt haben, sind daher ausgeschlossen.

Wir behalten uns ausdrücklich vor, das Muster ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen und übernehmen daher keine Gewähr und Haftung für die dauerhafte Verfügbarkeit der des Musters.

ⁱ Vertraulichkeit:

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;

- Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B.: Mandantenfähigkeit, Sandboxing;



- Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
 - Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).
- ii Integrität:
- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
 - Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;
- iii Verfügbarkeit und Belastbarkeit:
- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
 - Rasche Wiederherstellbarkeit;
 - Lösungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.
- iv Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:
- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
 - Incident-Response-Management;
 - Datenschutzfreundliche Voreinstellungen;
 - Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.