Anhang 1 zur Rahmenvereinbarung über die Auftragsverarbeitung gemäß Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO)

Deutsche Post Dialog Solutions GmbH
Koblenzer Str. 67
53177 Bonn

Dokumentation technische und organisatorische Maßnahmen des Auftragnehmers

1. Technisch Organisatorische Maßnahmen der Deutschen Post Dialog Solutions GmbH (DPDS)

Die nachfolgend beschriebenen Technisch Organisatorischen Maßnahmen (TOMs) gemäß Artikel 32 DSGVO gelten für die Leistungen der Deutschen Post Dialog Solutions GmbH, im Folgenden DPDS genannt. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die DPDS nachfolgende dargestellte TOMs, um ein dem Risiko der Leistungen angemessenes Schutzniveau zu gewährleisten. Die nachfolgend beschriebenen TOMs gelten auch für die von der DPDS eingesetzten Unterauftragnehmer. Zusätzliche Maßnahmen, die ausschließlich für die DPDS gelten, sind als solche gekennzeichnet.

2. Vertraulichkeit

Artikel 32 Absatz 1 Buchstabe b DSGVO.

2.1. Physische Zutrittskontrolle

Kein unbefugter Zugang zu Datenverarbeitungseinrichtungen, z.B. Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Mitarbeiter der Gebäudesicherheitsdienste und/oder für Eingangskontrollen, Alarmsysteme, Videoüberwachungssysteme.

2.1.1. Umgesetzte Maßnahmen

- Anweisungen für Maßnahmen zur Zutrittskontrolle.
- Sicherheitsschlösser mit Schlüsselverwaltung.
- Codekarten sowie Ausweisleser und Wachdienst für die Gebäude der DPDS.
- Zutrittsregelungen für betriebsfremde Personen (Zutritt nur in Begleitung).
- Schaffung von Sicherheitsbereichen und Beschränkung der Zutrittswege (Zutrittskontrolle, Verschließen der Räume).
- Ablage der zentralen Daten in Rechenzentren, die DIN ISO 27001 zertifiziert sind, bei Verarbeitung durch die DPDS.
- Gebäudesicherung
- Sicherung durch Alarmanlage.

2.2. Elektronische Zugangskontrolle

Keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung, z.B. (sichere) Passwörter, automatische Sperr- / Schließmechanismen, Zwei-Faktoren-Authentifizierung, Verschlüsselung von Datenträgern / Speichermedien.

2.2.1. Umgesetzte Maßnahmen

- Auf allen betrieblich relevanten IT-Systemen der DPDS ist ein Zugangskontrollsystem etabliert, das eine Authentisierung durch Abfrage einer Benutzer-ID und eines Passworts verlangt.
- Verbindliche Passwortrichtlinie bei der DPDS mit Anforderungen zu komplexen Passwörtern.
- Passwortregeln bei Konfiguration der DPDS-IT-Systeme werden, wenn technisch nicht anders abbildbar, über Dienstanweisung umgesetzt.
- Einsatz von Verschlüsselungsroutinen für Dateien bei der Übertragung und beim Transport.
- Besondere Kontrolle des Einsatzes von Utilities durch Installationsberechtigung auf Arbeitsplätzen der DPDS nur für Administratoren. Regelmäßiges Einspielen von Sicherheitspatches auf den Systemen.
- Abschließbarkeit der DV-Anlagen und -Geräte (z.B. PC) der DPDS.
- Ausgabe von Datenträgern nur an autorisierte Personen (mit Begleitpapieren, Auftragsquittungen).
- Kontrollierte Lagerung der Datenträger in einem Sicherheitsbereich (z.B. Tresore).
- Anweisung zur Bildschirmsperre beim Verlassen des Arbeitsplatzes – automatische Bildschirmsperre bei Inaktivität.
- Abschottung interner Netzwerke gegen ungewollte Zugriffe von draußen (Firewall).
- Absicherung der Übertragungsleitungen durch verschlüsselte Übertragung von Kundendaten. Auf Anforderung für streng vertrauliche Daten end2end-Verschlüsselung.

2.3. Interne Zugriffskontrolle (Nutzerrechte für den Zugriff auf und die Änderung von Daten)

Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System, z.B. Berechtigungskonzept, Zugriffsrechte auf Need-to-know-Basis, Zugangs- und Zugriffsprotokollierung.

2.3.1. Umgesetzte Maßnahmen

- Auf allen betrieblich relevanten IT-Systemen der DPDS ist ein Zugriffskontrollsystem etabliert, das für den folgerichtigen Schutz von Ressourcen sorgt, indem es die berechtigten Systembenutzer identifiziert und authentisiert, den Zugriff auf die Einrichtungen des Systems kontrolliert, die Integrität von Ressourcen schützt sowie die Benutzung von Ressourcen beschränkt.
- Regelung zur Erteilung, Verwaltung und Überwachung von Zugriffsberechtigungen.
- Mandanten- / Rollen-Trennung auf Anwendungsebene.

2.4. Trennung nach Zweck

Getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden, z.B. Unterstützung des Verantwortlichen zu mehreren Zwecken, Sandboxing-Technik.

2.4.1. Umgesetzte Maßnahmen

- Trennung von Produktion und Testsysteme (z.T. auch Staging bzw. Referenz-systeme).

2.5. Pseudonymisierung

Artikel 32 Absatz 1 Buchstabe a DSGVO, Artikel 25 Absatz 1 DSGVO

Eine Methode / Art, personenbezogene Daten so zu verarbeiten, dass die Daten nur mithilfe zusätzlicher Informationen einer bestimmten betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen sind dabei getrennt zu speichern und mit angemessenen technischen und organisatorischen Maßnahmen zu schützen.

2.5.1. Umgesetzte Maßnahmen

- Sofern Livedaten im Testsystem der DPDS verwendet werden müssen, werden diese anonymisiert oder pseudonymisiert.
- Sofern personenbezogene Daten nur noch für statistische Zwecke der DPDS benötigt werden, werden diese anonymisiert.

3. Integrität

Artikel 32 Absatz 1 Buchstabe b DSGVO

3.1. Kontrolle der Datenübermittlung

Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei deren elektronischer/m Übermittlung oder Transport, z.B. Verschlüsselung, Virtuelle Private Netze (VPN), elektronische Signaturen.

3.1.1. Umgesetzte Maßnahmen

- Vernichtung, Löschung oder Rückgabe von Dateien oder Datenträgern (z.B. Fehldrucke), spätestens 90 Arbeitstage nach Beendigung der Verarbeitung.
- Protokollierung der durch die DPDS ausgelösten Datenübermittlungen sowie der Empfänger bei Dateiübertragungen mittels sftp-logging.
- Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden bei durch die DPDS ausgelösten Dateiübertragungen gezielt feststellen zu können.
- Gesicherte Datenleitungen (VPN, SSL-Tunnel) zwischen der DPDS und deren Rechenzentren sowie auch den Unterauftragnehmern.

- Daten werden – sofern sie auf Datenträgern versandt werden – auf Wunsch des Auftraggebers und nach Absprache mit kryptographischen Verfahren verschlüsselt und ausschließlich über zuverlässige Transportunternehmen mit dokumentierter Übergabe befördert.
- Auf Anforderung end2end-Verschlüsselung für strengvertrauliche Daten.

3.2. Kontrolle der Dateneingabe

Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben bzw. in diesem geändert oder gelöscht werden, z.B. Protokolle, Dokumentenmanagement.

3.2.1. Umgesetzte Maßnahmen

- Organisatorisch festgelegte Zuständigkeit für die Dateneingabe.
- Die Prozesse der DPDS zur Datenänderung sind dokumentiert, weiterhin existiert ein fachliches Logging, aus denen u.a. Änderungszeitpunkte von Datensätzen hervorgehen.
- Sämtliche administrativen Tätigkeiten der DPDS werden geloggt und vor Veränderung geschützt.

4. Verfügbarkeit und Belastbarkeit

Artikel 32 Absatz 1 Buchstabe b DSGVO

4.1. Verfügbarkeitskontrolle

Prävention gegen versehentliche(n) oder absichtliche(n) Zerstörung oder Verlust, z.B. Back-up-Strategie (online / offline; vor Ort / außerhalb des Standortes), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldeverfahren und Notfallplanung.

4.1.1. Umgesetzte Maßnahmen

- Ablage der zentralen Daten der DPDS in Rechenzentren, die DIN ISO 27001 zertifiziert sind.
- Regelmäßige Durchführung von Datensicherungen.
- Lagerung der Sicherungskopien an besonders geschützten Orten außerhalb des Rechenzentrums.
- Prüfsummenverfahren bei der DPDS, wo etabliert.
- Brandschutzmaßnahmen
- Unterbrechungsfreie Stromversorgung (USV).
- Einsatz von Datenbank-Clustern.
- Datenspiegelung relevanter Datenträger.

4.2. Rasche Wiederherstellung

Artikel 32 Absatz 1 Buchstabe c DSGVO

4.2.1. Umgesetzte Maßnahmen

- Regelmäßige Überprüfung der Sicherungs- und Wiederherstellbarkeit.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO

5.1. Datenschutz- und Reaktionsmanagement

5.1.1. Umgesetzte Maßnahmen

- Betrieb eines Information Security Management System innerhalb der DPDS, welches wesentliche Teile des Datenschutzmanagements umfasst (z.B. Prozesse bei Datenschutzvorfällen, Prozesse bei Notfällen oder Krisen).

5.2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 25 Absatz 2 DSGVO

5.2.1. Umgesetzte Maßnahmen

- Privacy-by-design:

  Die Entwicklung neuer Systeme innerhalb der DPDS erfolgt unter Einbezug des betrieblichen Datenschutzbeauftragten.

- Privacy-by-default:

  Sofern Standardsoftware zum Einsatz kommt, werden Werkseinstellungen sofern durch die DPDS veränderbar, so eingestellt, dass diese Datenschutzfreundlich ausgestaltet sind.

5.3. Auftrags- oder Vertragskontrolle bei der DPDS

5.3.1. Umgesetzte Maßnahmen

- Verarbeitung durch Dritte bzw. Unterauftragnehmer nach Maßgabe von Artikel 28 DSGVO ausschließlich auf entsprechende Weisungen des Verantwortlichen.
- Klare und eindeutige vertragliche Vereinbarungen mit Dienstleistern.
- Strenge Kontrollen bei der Auswahl der Dienstleister.
- Regelmäßige Lieferantenaudits.

5.4. Organisationskontrolle

5.4.1. Umgesetzte Maßnahmen

- Zutrittsberechtigungen
- Zugangsberechtigungen
- Zugriffsberechtigungen: Kundendaten sind bei der DPDS vor unberechtigtem Zugriff mit einem Berechtigungskonzept nach Nutzergruppen geschützt.
- Datenübertragung:
  Datenübertragungen von Kundendaten werden grundsätzlich SSL-verschlüsselt vorgenommen.
- Verpflichtung der DPDS-Mitarbeiter auf das Datengeheimnis.
- Aufklärung und Schulung der DPDS-Mitarbeiter mit Arbeitsaufnahme.
- Bestellung eines betrieblichen Datenschutzbeauftragten gemäß Vorgaben des § 38 BDSG-neu.
- Einhaltung der Grundsätze zur Funktionstrennung und klare Verantwortungsbereiche.
- Anweisungen und Richtlinien zur Anwendungsentwicklung und Produktion bei der DPDS.
- Systemdokumentation
- Trennung von Test und Produktion.
- Regelungen zu Test und Freigabe.
- Regelungen zu System- und Programmprüfung bei der DPDS sowie zum Löschungskonzept. Anwendungen werden erst nach erfolgter Qualitätssicherung und Freigabe in Betrieb genommen.
- DPDS-Datensicherungskonzept, -plan und -katalog.
- Wartungs- und Reparaturarbeiten:
  Wartungsarbeiten finden in geplanten Wartungsfenstern statt.
- Dokumentation von IT-Verfahren, Software und IT-Konfiguration der DPDS:
  - Software:
    - Fachliche Beschreibung von Anwendungsfällen
    - Technische Konzeption / Architekturdokumentation (je nach Anwendung unterschiedlich im Umfang).
    - Releasedokumentation
    - Dokumentation von Testfällen / Testläufen.
  - Prozesse / IT-Verfahren
    - Dokumentation von Organisationsprozessen (u.a. Release- / Freigabeprozess / Inbetriebnahme, Anforderungsanalyse) mit definierten Rollen / Verantwortlichkeiten.
    - Issue- / Bugtracking.