Anlage 1

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO, § 64 BDSG (neu) 2018 Data Service GmbH

Vorgaben zur Datensicherheit

Data Service ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die im Rahmen der Auftragsdurchführung verwendeten Daten zu treffen. Diese Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Datenverarbeitung zu treffen. Diese Maßnahmen sollen Vertraulichkeit, Integrität, Verfügbarkeit der Daten bei Vertragsdurchführung sicherstellen

Organisatorische Vorgaben zur Gewährleistung der Datensicherheit

Data Service unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.

Data Service trifft zur Gewährleistung der Datensicherheit folgende Maßnahmen, deren Einhaltung durch entsprechende Kontrollen im Rahmen der organisatorischen Maßnahmen gewährleistet wird:

A. Vertraulichkeit und Integrität (Art. 32 Abs. 1 lit. B DSGVO)

Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter (Data Service) nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. **Zugangskontrolle, § 64 Abs. 3 Nr. 1 BDSG (neu)**
   (Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte)

1.1. Rechenzentrum

- Der Auftragnehmer regelt die Zutrittsberechtigung der eigenen Mitarbeiter über Tätigkeitsprofile, sodass nur Mitarbeiter mit entsprechender Qualifikation Zutritt zu den Räumen erhalten, die eine hohe Sicherheitsstufe besitzen, oder in denen Datenverarbeitungsanlagen stehen.
- Der Zutritt erfolgt unter Verwendung von Chipkarten und wird über zentrale Zutrittskontrollsysteme protokolliert. Zusätzliche Code-Nummern-Taster.
- Der Zutritt zum Rechenzentrum ist über einen separaten Eingang sowie über eine Alarmanlage mit direktem Ruf zum externen Sicherheitsdienst abgesichert. Das Gelände des Rechenzentrums ist zudem mit einer Zaunanlage und Videoüberwachung ausgestattet.
- Für den Standort des Rechenzentrums erfasst der zentrale Empfang sämtliche allgemeinen Besuche formularmäßig. Beim RZ-Betreiber sind sämtliche geplanten Rechenzentrums-besuche frühzeitig anzumelden.
- Mitarbeiter von Fremdfirmen erhalten nur Zutritt zu ihren persönlichen Sicherheitsbereichen. Besuche außerhalb der Dienstzeit finden nur in Begleitung des Sicherheitsdienstes statt.

1.2. Benutzer

- An- und Abmeldeprozedur mit Passwortverwaltung
- Regelung zum Entzug von Zugangsrechten und Zertifikaten bei Beendigung des Dienstverhältnisses oder internem Wechsel.

1.3. Netze

-Absicherung des Zugangs zu den Kommunikationsstrukturen direkt oder aus dem Internet durch Athentifizierungsverfahren
- Regelung zur Authentifizierung von Fernzugriffen
- Kein WLAN auf Produktivsystemen
- Fernzugang über nach dem aktuellen Stand der Technik verschlüsselte Internet-Verbindungen (virtuelle private Netzwerke – VPN)

1.4. Betriebssysteme

- Sicheres Anmeldeverfahren mit sicheren Passwörtern
- Eindeutige Benutzerkennung
- Einschränkung von Administrator-Diensten

1.5. Anwendungen

- Sicheres Anmeldeverfahren mit sicheren Passwörtern
- Eindeutige Benutzerkennung
- Passwortvergabe durch Benutzer

2. Datenträgerkontrolle, § 64 Abs. 3 Nr. 2 BDSG (neu)

(Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern)

2.1. Prozess zur Vergabe, Entzug und Kontrolle von Berechtigungen

2.2. Datenschutzgerechte Entsorgung von Testdrucken, Auswertungen etc. von im Hause des Auftragnehmers befindlichen Materialien.

3. Speicherkontrolle, § 64 Abs. 3 Nr. 3 BDSG (neu)

(Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten)

3.1. Protokollierung in der jeweiligen Anwendung

4. Benutzerkontrolle, § 64 Abs. 3 Nr. 4 BDSG (neu)

(Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte)

4.1. Sicheres Anmeldeverfahren mit sicheren Passwörtern

4.2. Eindeutige Benutzerkennung

4.3. Regelung zum Entzug von Zugangsrechten und Zertifikaten bei Beendigung des Dienstverhältnisses oder internem Wechsel.

5. Zugriffskontrolle, § 64 Abs. 3 Nr. 5 BDSG (neu)

(Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben)

5.1. Beim Auftragnehmer werden bedarfsgerechte Zugriffe mit speziellen Berechtigungen auf die Systeme definiert, und dadurch der Zugriff auf die Systeme geregelt.

5.2. Die Vergabe von Berechtigungen kann nur von bestimmten Mitarbeitern des Auftraggebers/Kunden beim Auftragnehmer angefordert werden. Der Service-Bereich des Auftragnehmers richtet die Berechtigungen entsprechend den Vorgaben des Auftraggebers ein. Z.B. Lesen, Verändern, Löschen von Daten, Definition des Funktionsprofils.

6. Übertragungskontrolle, § 64 Abs. 3 Nr. 6 BDSG (neu)

(Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können)

6.1. Nur durch die Applikation oder definierte Prozesse geregelt möglich. Kein direktes Einspeichern von Daten.

6.2. Protokollierung

7. Eingabekontrolle, § 64 Abs. 3 Nr. 7 BDSG (neu)

(Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind)

7.1. Protokollierung in der jeweiligen Anwendung

8. Transportkontrolle, § 64 Abs. 3 Nr. 8 BDSG (neu)

(Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden)

8.1. Datenschutzkonformes Löschen und Entsorgen von Festplatten

8.2. Kryptographische Verfahren (Datenverschlüsselung, SFTP)

8.3. Kein WLAN auf Produktivservern

8.4. Bei direkter Abholung von gedruckten Ergebnissen Dokumentation und Bestätigung durch den Auftraggeber/Kunden. Authentifizierung durch Kundenausweis. Die ordnungsgemäße Zuteilung bzw. Einziehung von Kundenausweisen obliegt dem Auftraggeber.

9. **Datenintegrität, § 64 Abs. 3 Nr. 11 BDSG (neu)**
   (Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können)

   9.1. Brandschutzkonzept

   9.2. Notfallhandbuch

   9.3. Server-Shutdown-Liste

10. **Trennbarkeit, § 64 Abs. 3 Nr. 14 BDSG (neu)**
    (Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können)

    10.1. Physikalische und Logische Trennung von Anwendungen

    10.2. Physikalische und logische Trennung bei der Datenhaltung

    10.3. Mandantenfähigkeit

    10.4. Trennung von Test- Entwicklungs- und Produktivsystemen

11. **Pseudonymisierung, Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO**
    (Pseudonymisierung bedingt die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen)

    11.1. Pseudonymisierung ist auf Grund des Geschäftsmodells nur durch den Auftraggeber möglich

    11.2. Die Produktivverarbeitung erfolgt auf Grund des Dienstleistungsvertrages mit den zur Verfügung gestellten Daten

B. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. **Wiederherstellbarkeit, Art. 32 Abs. 1 lit. c DSGVO; § 64 Abs. 3 Nr. 9 BDSG (neu)**
   (Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)

   1.1. Tägliches Backup aller Systeme (Virtuelle Maschinen)

   1.2. Prozess zur Aufnahme von Neusystemen in die Backuperstellung

2. **Zuverlässigkeit, § 64 Abs. 3 Nr. 10 BDSG (neu)**
   (Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden)

   2.1. Anwendungsspezifische Redundanzen bei Systemen und Datenbanken nach Vorgaben des Auftraggebers

3. **Verfügbarkeitskontrolle, § 64 Abs. 3 Nr. 13 BDSG (neu)**
   (Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind)

   3.1. Die Verfügbarkeit der angebotenen Dienste wird durch folgende Maßnahmen gewährleistet:
   - separates Rechenzentrum,
   - unterbrechungsfreie Spannungsversorgung,
   - Versorgung mit Notstrom bei längerfristigem Spannungsausfall,
   - redundante Netzwerkanbindung des Rechenzentrums,
   - regelmäßige Datensicherung und Überprüfung der Datensicherung,
   - regelmäßige Überprüfung der Haustechnik und Stromversorgung,
   - Klimaversorgung und Brandschutzmaßnahmen.
   - Verwendung von RAID Systemen

   3.2. Server- und Datenbankredundanzen gemäß Weisung des Kunden.

C. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

1. Datenschutz-Management

1.1. Beim Auftragnehmer gelten die Grundsätze:
Datenschutz ist Aufgabe des gesamten Unternehmens
Es werden datenschutzfreundliche Technologien eingesetzt, wo immer das möglich und wirtschaftlich ist.
Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein

1.2. Der Auftragnehmer legt Strategien fest hinsichtlich:
Zuweisung von Zuständigkeiten
Risikobewertung
Durchführung von Kontrollen
Sensibilisierung und Schulung der Mitarbeiter

1.3. Wenn immer das erforderlich ist, werden die eingesetzten Verfahren einer dokumentierten Datenschutz-Folgenabschätzung unterzogen, bestehend aus:
Schutzbedarfsfeststellung
Risikoanalyse
Sicherheitskonzept

1.4. Durchgeführte Verarbeitungstätigkeiten werden einheitlich und nachweisbar dokumentiert

1.5. Weisungen von Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert

1.6. Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert

1.7. Alle eingesetzten Auftragsverarbeiter werden eingehenden Prüfungen unterzogen. Dabei werden die gleichen Maßstäbe angesetzt, die für die eigene Verarbeitung gelten

2. Incident-Response-Management

2.1. Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

3.1. Es werden für den jeweiligen Verarbeitungszweck geeignete technische und organisatorische Maßnahmen getroffen, die jedem Auftraggeber im Rahmen der Vereinbarung einer Auftragsverarbeitung zugesichert werden. Spätere Änderungen dieser Maßnahmen können nur zu besseren Zuständen führen, niemals zu einer Verschlechterung.

3.2. Es gilt stets die höchste Schutzstufe bei der Erstellung neuer Objekte in der Berechtigungs- und Zugriffsverwaltung. So hat beispielsweise eine neu erstellte Kennung zunächst keinerlei Rechte im System und erhält diese erst, wenn ihr ein Profil (Sammlung von Rechten) zugeordnet wird.

3.3. Erstellte Auswertungsergebnisse und Listen – ob im Einzelfall oder fallübergreifend – können nur von daraufhin berechtigten Personen eingesehen werden.

4. Auftragskontrolle, § 64 Abs. 3 Nr. 12 BDSG (neu)

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

4.1. Der Auftragnehmer kontrolliert die Einhaltung der Datensicherheitsbestimmungen. Hierzu verpflichtet der Auftragnehmer seine Mitarbeiter zur Wahrung der datenschutzrechtlichen Vorgaben.

4.2. Auftragsnehmer und Auftraggeber verpflichten sich zur gegenseitigen Erstattung von Meldungen, wenn ein Verstoß oder ein Verdacht des Verstoßes gegen eine datenschutzrechtliche Bestimmung besteht.