# Anlage 1

# Technisch-organisatorische Maßnahmen zum Datenschutz nach Art. 32 DSGVO

Die Datenverarbeitung erfolgt ausschließlich auf den Servern in den Rechenzentren an den verschiedenen Standorten. Die Maßnahmen in den Bereichen Zutritts- bzw. Zugangskontrolle können daher je nach Standort abweichen, die Einhaltung des erforderlichen Schutzniveaus ist aber in jedem Fall sichergestellt.

Die Maßnahmen in den Bereichen Zugangskontrolle, Zugriffskontrolle und Weitergabekontrolle gelten für den Datenverkehr zwischen den Rechenzentren, die Zugriffe von Kunden auf die Systeme und für die Administration der Systeme durch Mitarbeiter von Byteplant.

## 1. Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Festlegung zutrittsberechtigter Personengruppen, Berechtigungskonzept | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 2 | Sicherung auch außerhalb der Arbeitszeit durch eine Alarmanlage und/oder Werkschutz | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 3 | Absicherung der Zutrittswege (Alarmanlage) | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 4 | Türsicherung (zum Beispiel elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner) | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 5 | Maßnahmen zur Objektsicherung (zum Beispiel Spezialverglasung, Alarmanlage, Absicherung von Schächten, Geländebewachung, Werkschutz) | **X** | durch jeweiligen Rechenzentrums-betreiber |

## 2. Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen in das EDV-System selbst:

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Festlegung differenzierter Zugangsregelungen (zum Beispiel für Beschäftigte, Firmenfremde) | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 2 | Verschließbarkeit von Datenverarbeitungsanlagen (zum Beispiel des Serverraums) | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 3 | Sicherung des Netzwerks gegen Zugriffe von außen (Firewalls, Intrusion Prevention System, Einrichtung einer demilitarisierten Zone) | **X** | |
| 4 | Sicherung von Bildschirmarbeitsplätzen (zum Beispiel Bildschirmsperre) | **X** | |
| 5 | Funktionelle und/oder zeitlich beschränkte Nutzung von Systemen und Identifizierungsmerkmalen (Beenden einer Sitzung nach festgelegter inaktiver Zeit; nach | **X** | |

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| | mehrmaliger falscher Passworteingabe) | | |
| 6 | Regelung der Benutzerberechtigung | X | |
| 7 | Verschlüsselung von Netzwerken (zum Beispiel VPN; passwortgesicherte WLANs) | X | |
| 8 | Verschlüsselung der Fernwartung, -zugriffs | X | |

## 3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Festlegung der Zugriffsberechtigung auf Daten durch ein Berechtigungskonzept | X | Nur die Administratoren sind zugriffsberechtigt. |
| 2 | Identifizierung der zugriffsberechtigten Personen gegenüber dem Datenverarbeitungssystem (zum Beispiel durch Passwörter, Zugangscodes) | X | |
| 3 | Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung (je nach Rollenzuweisung: Lesen, Schreiben, Löschen) | X | |
| 4 | Rahmenvereinbarung bzw. Dienstanweisung zum Umgang mit Passwörtern, mobilen Endgeräten, privaten Emails; Bildschirmsperren | X | Geregelt per Rahmenvereinbarung bzw. Dienstanweisung an alle Mitarbeiter:<br>- Regelung zum Umgang mit Passwörtern<br>- keine Nutzung mobiler Endgeräte<br>- Verwendung von Bildschirmsperren<br>- keine Nutzung von dienstlichen Email-Accounts für private Zwecke. |

## 4. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Verschlüsselung von Daten und Verbindungen (zum Beispiel verschlüsselte Verbindung über das Internet) | X | |
| 2 | Berechtigungskonzept (Festlegung autorisierter Personen zur Datenübergabe) | X | |
| 3 | Kontrolle durch Beschäftigte (Vier-Augen-Prinzip) | X | |
| 4 | Festlegung der Bereiche, in denen sich Datenträger befinden müssen oder befinden dürfen | | Es werden keine externen Datenträger benutzt. |
| 5 | Absicherung der Bereiche, in denen sich Datenträger befinden zum Beispiel bei Transport/Übergabe | | Es werden keine externen Datenträger benutzt. |
| 6 | Festlegung der Personen, die aus diesen Bereichen Datenträger entfernen dürfen | | Es werden keine externen Datenträger benutzt. |
| 7 | Differenzierte Verwaltung von Datenträgern, Bestandskontrolle | | Es werden keine externen Datenträger benutzt. |
| 8 | Dokumentation zu den Stellen, an die eine Übermittlung vorgesehen ist sowie der Übermittlungswege und Übergabe | X | |
| 9 | Kundenkommunikation per Email erfolgt ausschließlich über Office-Desktops. Mobile / private Endgeräte sind nicht zugelassen. | | Geregelt per Dienstanweisung an alle Mitarbeiter. |
| 10 | Löschung von Datenresten vor Datenträgeraustausch | X | Überschreibung |

## 5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Kennzeichnung erfasster Daten (zum Beispiel Datum und Anwender-ID, Inhalt) | | Die Dateneingabe erfolgt ausschließlich durch den Auftraggeber. |
| 2 | Organisatorische Festlegung der Zuständigkeiten für die Eingabe von Daten | | Die Dateneingabe erfolgt ausschließlich durch den Auftraggeber. |
| 3 | Regelung der Zugriffsberechtigungen | X | |
| 4 | Regelung zu Aufbewahrungsfristen für Revision und andere Nachweiszwecke | | Es werden keine Daten dauerhaft gespeichert;<br>Daten werden nach der Verarbeitung gelöscht und überschrieben. |

## 6. Auftragskontrolle

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

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer (vgl. Art. 28 Abs. 3 DSGVO) | **X** | |
| 2 | Regelung der Rechte und Pflichten des Auftragnehmers und Auftraggebers | **X** | |
| 3 | Prozess zur Erteilung und/oder Befolgung von Weisungen | **X** | |

## 7. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Festlegung von Verantwortlichkeiten | **X** | |
| 2 | Informieren der Beschäftigten über Notfallpläne und Durchführung von Tests und Übungen | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 3 | Datensicherungs-/Backup-Konzepte | | Kundendaten sind aus Datenschutzgründen vom Backup ausgeschlossen. |
| 4 | Regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen | **X** | durch jeweiligen Rechenzentrums-betreiber |
| 5 | Überwachung der Betriebsparameter von Rechenzentren | **X** | durch jeweiligen Rechenzentrums-betreiber |

## 8. Trennungsgebot

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung. Eine logische Trennung ist ausreichend.

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Trennung von Mandantendaten auf IT-Systemen | X | 1) auf Rechenzentrums-ebene:<br>durch den jeweiligen Rechenzentrums-betreiber<br><br>2) auf Systemebene:<br>Batch: Auftrags-ID<br>Online API: API Key |
| 2 | Funktionstrennungen | X | |
| 3 | Trennung von Entwicklungs-, Test- und Produktivsystem | X | |
| 4 | Regelungen zur Programmierung | X | |
| 5 | Regelungen zur System- und Programmprüfung | X | |

## 9. Evaluierung Art. 32 Abs. 1 lit. D DSGVO; Art. 25 Abs. 1 DSGVO

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Datenschutz-Management | X | |
| 2 | Auditierung durch den Datenschutzbeauftragten | X | jährlich und ggf. zusätzlich bei wesentlichen Änderungen |
| 3 | Regelmäßige Schulung der Mitarbeiter | X | |

## 10. Sonstige Maßnahmen

| # | Empfohlene Maßnahmen | Maßnahme umgesetzt | Anmerkungen |
|---|---|---|---|
| 1 | Vorhandensein von Konzepten, Richtlinien und Arbeitsanweisungen (zum Beispiel Datenschutzkonzept) | X | |
| 2 | Verpflichtung der Mitarbeiter auf die Vertraulichkeit | X | |
| 3 | Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) | X | |
| 4 | Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO) | X | |
| 5 | Meldeprozess für Datenschutzverletzungen | X | |