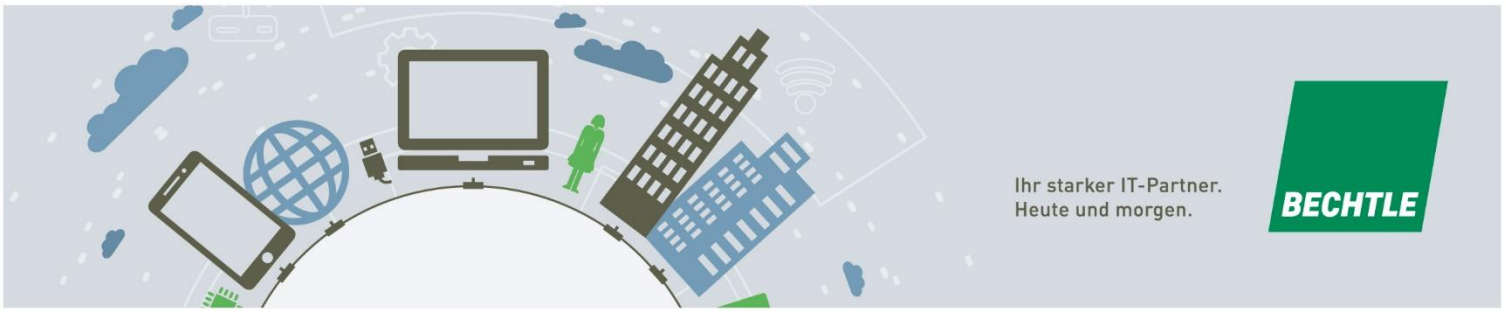


# Datenschutz- und Datensicherheitskonzept

## Technische und organisatorische Maßnahmen

**planetsoftware GmbH**

Meidlinger Hauptstraße 73
1120 Wien

**vorgelegt von**

**planetsoftware GmbH**

Meidlinger Hauptstraße 73
1120 Wien

# Inhalt

# 1 Vorwort

Das Dokument beschreibt die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Auftraggeber und Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutz- und Datensicherheitskonzept der Bechtle AG dar.

## 1.1 Geltungsbereich

Die beschriebenen technischen und organisatorischen Maßnahmen gelten für die Standorte in Wien, Wels, Innsbruck und Graz.

# 2 Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DS-GVO.

Die EU-DS-GVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen.

Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit.

Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- **Vertraulichkeit**:
  Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- **Integrität:**
  Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- **Verfügbarkeit:**
  Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- **Belastbarkeit:**

  Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst Widerstandsfähig ausgestaltet sein müssen.

# 3 Vertraulichkeit

Geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit werden, unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung, der Implementierungskosten und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen. Hiermit wird ein dem Risiko angemessenes Schutzniveau gewährleistet.

## 3.1 Zutrittskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

### 3.1.1 Zentrale Datenverarbeitungsanlagen

Objektsicherung
- Die zentralen Datenverarbeitungsanlagen befinden sich in einem Serverraum am Standort Wien.

Sicherheitszonen
- Der Serverraum ist mit strikter Zutrittsbeschränkung ausgestattet.
- Alarmanlage im Vorbereich (Gang)

Art der Zutrittskontrolle
- Zutrittskontrolle mittels Schlüssel (getrennt von Büros)

Regelung der Zutrittsberechtigungen
- Zutrittsregelungen für Mitarbeiter

Personenkontrolle
- Anmeldung und Begleitung von Besuchern und Firmenfremden
- Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen

### 3.1.2 Büroräume

Objektsicherung
- Die Büros befinden sich in angemieteten Räumen an den Standorten.

Sicherheitszonen
- Die angemieteten Büroräume sind räumlich von anderen Firmen getrennt.

Art der Zutrittskontrolle
- Schlüssel
- Schließregelung (verschlossene Türen bei Abwesenheit)

Regelung der Zutrittsberechtigungen
- Zutrittsregelungen für Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Wartungs-/ Reinigungspersonal, Lieferanten, Boten usw.)
- Festlegung befugter Personen (bezogen auf Zonen und Zeiten) – speziell für IT-Raum.
- Berechtigungen für Gäste nicht erforderlich; immer Begleitung durch Mitarbeiter
- Regelung beim Ausscheiden und Wechseln von Berechtigten

Personenkontrolle
- Anmeldung und Begleitung von Besuchern und Firmenfremden
- Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen

## 3.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

### 3.2.1 Regelung der Zugangsberechtigungen

- Regelungen für die Vergabe und Verwaltung von Zugangsberechtigungen
- Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- Zugangsberechtigte weisen sich durch Benutzerkennung und Passwort aus
- Regelung der Verwendung von Passwörtern
- Regelung für Sperrung des Arbeitsplatzrechners beim Verlassen
- Single Sign-On in Teilbereichen
- Berechtigungen (Kontenaktivierung) für temporäre Mitarbeiter/ Externe sind zeitlich befristet
- Regelung beim Ausscheiden und Wechseln von Berechtigten
- Regelungen bei Verlust (Vergessen) des Passwortes/ Passwörter
- Trennen der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen
- Getrennte Internet Infrastruktur für Besucher

### 3.2.2 Zusätzliche Maßnahmen beim Fernzugang

- Regelung für die Benutzung des Anschlusses, insbesondere bei Benutzung durch Dritte
- Festlegung der Personen, die zur Anmeldung von außerhalb befugt sind
- Netzzugangssicherungen durch Hard- und Softwaremaßnahmen – ausschließlich
- VPN-Zugänge mit Token / PIN 2-Wege Authentifizierung
- Regelungen bei Fernadministration und Fernwartung (Fernwartungskonzept)
- Verhinderung des unberechtigten Zugriffs aus dem Internet (Firewall)

### 3.2.3 Protokollierung von Zugängen

- Nachweis der Benutzung von DV-Systemen (Protokollierung der Zugänge)
- Protokollierung der fehlgeschlagenen Zugangsversuche (Entsperren eines Benutzers)
- Protokollierung der Vergabe/ Änderung von Zugangsberechtigungen

## 3.3 Zugriffskontrolle / Benutzerkontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

### 3.3.1 Berechtigungskonzept

- Nachweis der Benutzung von DV-Systemen (Protokollierung der Zugänge)
- Protokollierung der fehlgeschlagenen Zugangsversuche (Entsperren eines Benutzers)
- Protokollierung der Vergabe/ Änderung von Zugriffsberechtigungen

#### 3.3.2 Zugriffsschutz

- Passwortschutz bei Dateien nach Bedarf
- Einsatz von Verschlüsselungsroutinen/ Dateiverschlüsselung (Notebooks über Geräteverschlüsselung verschlüsselt)
- Trennung von Test- und Produktionsbetrieb (sofern erforderlich)
- „Mobile Device Management-System“

#### 3.3.3 Aufbewahrung bei Verwendung von Datenträgern

- Aufbewahrung in Zonen, die durch Schlüssel gesichert sind
- Fachkundige Akten- und Datenträgervernichtung (Aktenvernichter)
- Nicht-reversible Löschung von Datenträgern

#### 3.3.4 Protokollierung von Zugriffen

- Protokollierung von Lesezugriffen auf die Datensicherungen
- Protokollierung der Vergabe / Änderung von Zugriffsberechtigungen

### 3.4 Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

**Maßnahmen**

- Logische Trennung der Daten
- Mandantenfähigkeit von Anwendungen (sofern erforderlich)
- Innerbetriebliche Vorgaben für die Datenerhebung und die -verarbeitung
- Speicherung der Datensätze in getrennten Datenbanken (sofern erforderlich)
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Dokumentation der Verarbeitungsprogramme
- Dokumentation der Datenerhebungszwecke

### 3.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne weitere Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen den entsprechenden technischen und organisatorischen Maßnahmen.

**Maßnahmen**

- Pseudonymisierungen werden vom Auftragnehmer nur weisungsgebunden im Einzelfall realisiert.

## 4 Integrität

Die Richtigkeit der verarbeiteten personenbezogenen Daten ist zu gewährleisten. Unzulässige Änderungen müssen identifiziert und korrigiert werden können.

### 4.1 Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

#### 4.1.1 Regelung der elektronischen Übertragung

- Festlegung der Personen, die zur Übermittlung befugt sind (Berechtigungskonzept)
- Verschlüsselung der Daten bei der Übertragung (z. B. SSL/TLS)
- Authentisierung bei Mails (digitale Signatur) in Teilbereichen
- Protokollierung der Datenübermittlung und der Empfänger (bei Bedarf)
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB Stick, Mobiltelefon)

#### 4.1.2 Regelung bei der Speicherung auf Wechseldatenträgern

Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist grundsätzlich nicht vorgesehen. Im Ausnahmefall werden ausschließlich verschlüsselte USB-Sticks verwendet.

#### 4.1.3 Regelungen des Transports von Datenträgern

Transport von Datenträgern mit personenbezogenen Daten wird ausschließlich durch betriebszugehörige Boten, gesicherte Transportverhältnisse oder eine sonstige sichere Versendeform durchgeführt. Datenträger sind stets verschlüsselt.

### 4.2 Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

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

**Maßnahmen:**
- Zuständigkeiten für die Dateneingabe sind festgelegt (einschließlich Regelung der Stellvertretung)
- Protokollierung aller Eingaben, Veränderungen oder Löschungen personenbezogener Daten (in Teilbereichen)

## 5 Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

**Maßnahmen:**

### 5.1 Erstellung und Verwahrung von Sicherheitskopien

- Generelles Datensicherungskonzept
- Kontrollierte und regelmäßige Sicherung der Benutzerdateien, Datenbanken
- Namenskonventionen für Sicherungsdateien
- Kennzeichnung der Datenträger
- Verwendung des Schreibschutzes bei Datenträgern (logisch)
- Bestandsverzeichnis der Sicherungskopien (Dateien, Datenträger)
- Bestandskontrolle von Datenträgern
- Protokollierung von Sicherheitsspeicherungen
- Lagerung von Kopien an besonders geschützten Orten (Offsite an einen anderen Standort)
- Festlegung von Aufbewahrungsfristen

## 5.2 Gewährleistung des laufenden Betriebes

Die Infrastruktur im IT-Serverraum ist wie folgt gewährleistet:

### 5.2.1 Unterbrechungsfreie Stromversorgung

- Unterbrechungsfreie Stromversorgung mit ausreichender Kapazität ist vorgeschaltet;
- Ordnungsgemäße Funktionsfähigkeit wird durch regelmäßige Tests sichergestellt;
- Monitoring.

### 5.2.2 Brandschutz

- Brandmeldeanlage in Betrieb;
- Auf eine Brandlastreduzierung wird geachtet.

### 5.2.3 Klimatisierung

- Klimaanlage im Mietumfang enthalten;
- Zentrales Monitoring-System mit definierter Alarmweiterleitung.

### 5.2.4 Anbindung Internet

- Redundante Internetanbindung (teilweise automatisiert);
- Anbindung über unterschiedliche Provider.

## 5.3 Organisatorische Maßnahmen

- Funktionstrennung zwischen Fachabteilung und DV-Abteilung
- Sicherheitsrichtlinien sowie sicherheits- und datenschutzspezifische Arbeitsanweisungen existieren, wurden verkündet und werden kontrolliert;
- Vorgaben für Verfahrens- und Programmdokumentation;
- Eingesetzte Hard- und Software wird regelmäßig überprüft;
- Vorhandensein ausreichender Personalressourcen;
- Anwender werden geschult;
- Zentrale und einheitliche Beschaffung von Hard- und Software;
- Erlass von Dienstanweisungen und Sicherheitsrichtlinien;
- Vorhandensein ausreichender Personalressourcen in der DV-Abteilung;
- Angemessene Schulung der Anwender.

# 6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

## 6.1 Datenschutz-Management

Die umfangreichen Pflichten und Anforderungen der EU-DS-GVO erfordern eine ganzheitliche Strategie nach einem strukturierten Ansatz und ein entsprechendes Managementsystem. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Datenschutz-Managements.

**Maßnahmen**

- Datenschutz-Management gemäß der Datenschutzrichtlinie der Bechtle-Gruppe
- Datenschutzorganisation etabliert;
- Über Datenschutzstrategie wird ein strukturierter Ansatz verfolgt;
- Etablierte Prozesse sehen die Einbindung des Datenschutzbeauftragten vor

- Datenschutzrelevante Richtlinien und Arbeitsanweisungen werden verkündet und die Einhaltung kontrolliert;
- Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren.

## 6.2 Incident-Response-Management

Um im Bedarfsfall eines Vorfalls reagieren zu können, sind einschlägige Meldewege zu definieren und Verantwortlichkeiten festzulegen.

**Maßnahmen**

- Meldeprozess gemäß der Datenschutzrichtlinie der Bechtle-Gruppe
- Meldepflicht bei Datenpannen und Sicherheitsvorfällen
- Mitarbeiter sind entsprechend geschult;
- Meldestellen und Meldewege für Vorfälle- und Sicherheitsvorfälle sind definiert;
- Geordnete Behandlung ist sichergestellt;
- Dokumentation wird gepflegt;
- Gewonnene Erfahrungswerte fließen in die weitere Ausgestaltung und Verbesserung der Prozesse ein;

## 6.3 Datenschutzfreundliche Voreinstellungen

Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten nur nach den jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit).

**Maßnahmen**

- Privacy by Design und Default gemäß der Datenschutzrichtlinie der Bechtle-Gruppe
- Frühzeitige Einbindung der lokalen bzw. des zentralen Datenschutzkoordinators bei Projekten
- Durch kontinuierlichen Sensibilisierungs- und Schulungsprozess im Rahmen des Datenschutzmanagements sind die Mitarbeiter behutsam im Umgang mit personenbezogenen Daten;

## 6.4 Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

**Maßnahmen**

- Es besteht ein schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer
- Der Auftraggeber erteilt dem Auftragnehmer die Weisungen in Schriftform
- Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers
- Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden
- Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen; Gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern
- Interner Prozess stellt sicher, dass notwendige Verträge zur Auftragsdatenverarbeitung abgeschlossen werden.