bisping & bisping

Stand 09/2023

Technische und organisatorische Maßnahmen nach § 64 BDSG und Art. 32 DS-GVO sowie dessen Anlage:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Zielsetzung:

Es sollen nur Befugte zu den Räumen mit Datenverarbeitungsanlagen haben, mittels derer personenbezogene Daten verarbeitet oder genutzt werden.

Geltungsbereich:

Die Vertragsparteien sind für die zu treffenden Maßnahmen in ihrem jeweiligen Herrschaftsbereich grundsätzlich selbst verantwortlich. Dies gilt auch bei der Auftragsverarbeitung.
In Fällen der AV ist der Auftraggeber dafür verantwortlich, dass die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen eine zum Schutz der verarbeiteten Daten angemessene Sicherheit bieten. Aus diesem Grund sind sie im Folgenden zu spezifizieren.

Umgesetzte Maßnahmen:

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten

- Zutrittskontrollsystem
  - Personalisiertes Zutrittskontrollsystem mit Zwei-Faktor Authentifizierung für Gebäude- und Rechenzentrumszugang
  - Persönlicher Empfang während der Geschäftszeiten
  - Besucherliste mit Ausweisausgabe oder Abholung und Begleitung durch Personal, Dokumentation der Ein- und Ausgangszeiten sowie Ansprechpartner
  - Protokollierung der Schließvorgänge
  - Rack-Schließung
  - Absicherung von Gebäudeschächten
  - Sorgfältige Auswahl von Reinigungspersonal
  - Sorgfältige Auswahl von Wachpersonal
- Schlüssel / Schlüsselvergabe
  - Protokollierung der Schlüssel- und Keycard-Vergaben
- Überwachungseinrichtung
  - Mehrstufiger Perimeter-Schutz für Grundstück und Gebäude mit Anbindung und Überwachung durch den Sicherheitsdienst
  - Videoüberwachung sicherheitsrelevanter Bereiche

- Türsicherung
    - Elektronische Türöffner und Öffnungskontrolle zu sicherheitsrelevanten Bereichen

1.2 Zugangskontrolle

Zielsetzung:

Mit den Maßnahmen der Zugangskontrolle sollen nur Befugte Zugang zu den Datenverarbeitungseinrichtungen haben. Hier geht es nicht um die körperliche Zutrittskontrolle nach 1.1, sondern um den technischen / organisatorischen Zugang zu Datenverarbeitungssystemen bzw. deren Nutzungsmöglichkeit.

Geltungsbereich:

Es sind alle Personen einzubeziehen, die Datenverarbeitungsanlagen nutzen.

Umgesetzte Maßnahmen:

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) hinsichtlich der Benutzeridentifikation und Authentifizierung

- Personalisierte Zugänge berechtigter Personen
- Mindestanforderung an Passwort: 10 Zeichen, keine Trivialpasswörter; das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten
- Protokollierung der Zugriffe
- Systempasswörter werden generiert und verschlüsselt gespeichert
- Systembenutzer werden nur benutzt, sofern zwingend notwendig
- Weitergabe von Passwörtern ist verboten
- Zugänge für administrative Vorgänge erfolgen immer verschlüsselt (VPN, SSH, HTTPs, etc.)
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technonlogien bei der Übertragung von Daten
- Sperren externer Schnittstellen (USB, etc.)
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von zentraler Smartphone-Administrations-Software (z.B zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall
- Getrennte Verwendung von Benutzer- und Administratorenkonten
- Zwei-Faktor-Authentifizierung
- Automatische Bildschirmsperre bei Inaktivität

1.3 Zugriffskontrolle

Zielsetzung:

Ziel der Zugriffskontrolle ist es, mithilfe geeigneter Maßnahmen sicherzustellen, dass im Rahmen der Datenverarbeitung durch die MitarbeiterInnen nur auf die personenbezogenen Daten zugegriffen werden kann, für die sie eine Zugriffsberechtigung besitzen. Dritte dürfen keinen unbefugten Zugriff auf die Daten hinsichtlich Verarbeitung, Nutzung und Speicherung haben und auch eine unbefugte Entfernung der Daten darf nicht möglich sein.

Geltungsbereich:

Die Zugriffskontrolle ist bei jeglicher EDV-Anwendung durchzuführen; somit auch für den PC-Bereich.

Umgesetzte Maßnahmen:

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung

- Definiertes und differenziertes Rollen- und Berechtigungskonzept
- Kenntnisnahme / Zugriff auf Informationen ist nur entsprechend des Rollen- und Berechtigungskonzeptes möglich
- Protokollierung nicht autorisierter Zugriffsversuche
- Veränderung von Informationen ist nur entsprechend des Rollen- und Berechtigungskonzeptes möglich
- Löschung ist nur entsprechend des Rollen- und Berechtigungskonzeptes möglich
- Aktenvernichtungsprozess inkl. Verschlussbehälter
- Datenträgervernichtung gemäß DIN 60399
- Regelungen zum Aufgeräumten Arbeitsplatz (Clear-Desk) und automatische Bildschirmsperre bei Inaktivität
- Abschließbare Schränke und Rollcontainer
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o. Ä.)
- Sichere Aufbewahrung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Protokollierung der Aktenvernichtung

1.4 Trennungsgebot

Zielsetzung:

Mit dieser Anforderung soll gewährleistet werden, dass Daten nur zu dem Zweck, zu dem sie bei der Erfassung erhoben wurden, verarbeitet werden dürfen. Der Zweck für den die Daten erhoben wurden, darf nicht geändert werden.
Aus diesem Grund ist es wichtig, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, vollständig getrennt voneinander gespeichert werden. (Zweckbindungsgrundsatz)

Geltungsbereich:

Diese Vorschrift gilt sowohl für Daten, die von der verantwortlichen Stelle selbst, als auch für die, die durch Dritte im Auftrag erhoben wurden.

Umgesetzte Maßnahmen:

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken

- Funktionstrennung von Entwicklungs-, Test- und Produktivumgebungen
- Zugriffssicherung auf Daten durch Berechtigungskonzept
- Interne Mandantenfähigkeit bei allen Applikationen, bei denen personenbezogene Daten verarbeitet werden

Berechtigungskonzept

- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Zielsetzung:

Die Verarbeitung personenbezogener Daten soll derart erfolgen, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

Geltungsbereich:

Diese Vorschrift gilt sowohl für Daten, die von der verantwortlichen Stelle selbst, als auch für die, die durch Dritte im Auftrag erhoben wurden.

Umgesetzte Maßnahmen:

Alle IP-Adressen werden soweit möglich verkürzt gespeichert. Darüber hinaus werden personenbezogene Daten durch die beschriebenen Zugangs- und Zugriffskontrollen und weitere Verschlüsselungen geschützt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Zielsetzung:

Ziel der Weitergabekontrolle ist es, durch geeignete Maßnahmen zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung und beim Transport per Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Der Gesetzgeber empfiehlt hierzu insbesondere die Maßnahme der Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Der Einsatz eines Verschlüsselungsverfahrens ist jedoch dann nicht zwingend notwendig, wenn durch die getroffenen Schutzmaßnahmen eine der Verschlüsselung vergleichbare Sicherheit erreicht wird. Sofern die getroffenen Schutzmaßnahmen

diese Sicherheit nicht erreichen, wird die Verwendung der dem Stand der Technik entsprechenden Verschlüsselungsverfahren empfohlen.

Geltungsbereich:

Die Weitergabekontrolle gilt sowohl für die Datenweitergabe an Dritte, als auch für den innerbetrieblichen Datentransfer und zwischen Auftraggeber und Auftragnehmer bei der Auftragsverarbeitung.

Umgesetzte Maßnahmen:

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger

- Systeme werden durch Firewallsysteme geschützt (Soft- und ggf. Hardware)
- Weitergabe von vertraulichen und personenbezogenen Daten erfolgt verschlüsselt (VPN, SSH, HTTPs, etc.)
- Einsatz von technischen Systemen zur Kontrolle von Schnittstellen (z.B. USB)
- Entsorgung von vertraulichen Dokumenten via Aktenvernichter
- Vernichtung von Datenträgern via zertifizierte Entsorger
- Verschlüsselung physischer Datenträger bei Transport

2.2 Eingabekontrolle

Zielsetzung:

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass die näheren Umstände der Dateneingabe nachträglich überprüft und festgestellt werden können.

Geltungsbereich:

Die Gewährleistung der erforderlichen Kontrollmaßnahmen obliegt sowohl dem Auftraggeber, als auch dem Auftragnehmer.

Umgesetzte Maßnahmen:

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind

Über die Werkzeuge der Nutzerverwaltung und der damit verbundenen Rechteverwaltung ist nachvollziehbar, wer Neueingaben, Änderungen oder das Löschen personenbezogener und vertraulicher Informationen veranlassen kann.

- Verwendungen von personenbezogenen Accounts wann immer möglich
- Trennung von Benutzer- und Administratorenkonten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Zielsetzung:

Ziel der Verfügbarkeitskontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass geschützte Daten nicht durch Zufälligkeiten zerstört werden oder verloren gehen.

Geltungsbereich:

Es ist die Gesamtheit des Datenverarbeitungssystems einzubeziehen – sowohl Menschen, als auch Programme und Materialien.

Umgesetzte Maßnahmen zur Datensicherung (physikalisch / logisch):

- Datenspeicherung des Serverbetriebs im hochverfügbaren Sicherheitsrechenzentrum
- Datensicherheit in separaten Brandabschnitten bzw. weiteren Rechenzentren
- Notfallhandbuch für Ausfallszenarien inkl. Wiederanlaufplan
- Backup -/ Restorekonzept zur Datenwiederherstellung vorhanden
- Backupkonzept sowie regelmäßige Wiederherstellungtests. Neben täglichen und wöchenlichten Online-Backups (georedundant) werden auch monatliche Offline-Backups für den Zeitraum von 12 Monaten gehalten.
- Testen von Datenwiederherstellung
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Zielsetzung:

In regelmäßigen Abständen, jedoch mind. jährlich, soll durch ein geregeltes Verfahren sichergestellt und überprüft werden, ob die getroffenen technischen und organisatorischen Maßnahmen noch wirksam sind.
Hierdurch soll das Datenschutz-Risiko minimiert werden, indem Angriffsstellen lokalisiert und behoben werden. Dies ist auch aufgrund der ständigen technologischen Weiterentwicklung unbedingt erforderlich.

Geltungsbereich:

Die Vertragsparteien sind für die zu Umsetzung des Verfahrens in ihrem jeweiligen Herrschaftsbereich grundsätzlich selbst verantwortlich. Dies gilt auch bei der Auftragsverarbeitung.

Umgesetzte Maßnahmen:

4.1 Datenschutz-Management

Die wesentlichen Prozesse zum Datenschutz-Management sind definiert und unterliegen einer kontinuierlichen Verbesserung.

4.2 Incident-Response-Management

Incident-Response-Management ist in unserem ISMS nach ISO27001 abgebildet und unterliegt einer kontinuierlichen Verbesserung. Alle relevanten Risiken sind im geschäftslichen Kontext ermittelt und nach Eintrittswahrscheinlichkeit und Schadensausmaß bewertet. Ein Notfallkonzept liegt vor und legt Maßnahmen und Verantwortlichkeiten für Wiederanlauf bzw. Wiederherstellung fest.

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

Anwenderspezifische Einstellungen in standardisierten Verarbeitungssystemen werden soweit möglich so gesetzt, dass ein zwingendes Eingreifen einer Person zur Ausführung eines personenbezogenen Datenabrufes notwendig ist und hierbei nur solche Daten zur Verfügung gestellt werden, welche für den jeweiligen Verarbeitungszweck definiert sind. Dies gilt ebenso für interne Tools und Verfahren.

4.4 Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer
Bei der Verarbeitung von personenbezogenen Daten im Rahmen einer Auftragsdatenverarbeitung wird sichergestellt, dass die Datenverarbeitung auf Weisung des Kunden stattfindet und nur im Rahmen dieser Weisungen stattfindet. Eine darüber hinaus gehende unbefugte Datenverarbeitung ist den Mitarbeiter/innen vertraglich durch eine schriftliche Datenschutzvereinbarung untersagt. Der Inhalt der Weisungen eines Kunden wird den mit der im Rahmen des jeweiligen Auftraggebers betrauten Mitarbeiter/innen verbindlich mitgeteilt.
Alle Mitarbeiter, die mit der Bearbeitung der Daten betraut sind, wurden auf das Datengeheimnis verpflichtet und unterliegen regelmäßigen Schulungen und Unterweisungen in Belangen des Datenschutzes durch den bestellten Datenschutzbeauftragten.

Mit externen Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, sind konforme Vereinbarungen nach den Datenschutzgesetzen abgeschlossen worden.

4.5 Information Security Management System (ISMS)

Des weiteren wird ein internes Information Security Management System nach ISO 27001, das dazu dient die Informationssicherheit zu definieren, zu steuern, zu überwachen und kontinuierlich zu optimieren, betrieben. Ein wichtiger Bestandteil des ISMS ist ein dokumentiertes internes IT-Sicherheitskonzept nach TKG §109, regelmäßig geprüft und genehmigt durch die BNetzA (Bundesnetzagentur).