Direkt.
Dialog.
Digital.

Anlage 1 – Technisch-organisatorische Maßnahmen

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

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren.
Es existieren bei ODS folgende Maßnahmen zur Zutrittskontrolle:

- Gesicherte Zugänge mit elektrischen Türschließern. Jeder Mitarbeiter erhält Zutritt in die Betriebsräume von ODS mit individuell, je nach Zugangsberechtigung eingerichtetem Transponderschlüssel.
- Protokollierte Ausgabe der Transponderschlüssel
- Schriftliche Betriebsanweisung für Schlüsselregelung für die Produktionsräume
- Anwesenheitsaufzeichnungen über ein elektronisches Zeiterfassungssystem
- Beaufsichtigter Eingang für An- und Ablieferung
- Sicherung des Büroeingangsbereiches mit Kamera inkl. Aufschaltung zu externer Sicherheitsfirma
- Das Gelände wird durch regelmäßige Rundgänge der externen Sicherheitsfirma und Verschließen der Toranlage zum Innenhof ab 22.00 Uhr gesichert.
- Schriftliche Festlegung für Umgang mit betriebsfremden Personen.

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Es existieren bei ODS folgende Maßnahmen zur Zugangskontrolle:

- Datenträger des Datenservers nur für berechtigte Personen mit Transponderschlüssel zugänglich
- Individuelle Benutzerkennung. Authentisierung mit Benutzername und persönlichem Passwort
- Eingerichtete Passwortanforderung mit erzwungener Mindestlänge (8), Maximalter (60 Tage) und Komplexität (muss aus Sonderzeichen, Groß- und Kleinbuchstaben und Ziffern bestehen), sowie Historie (6) für Passwörter.
- Getrennte Benutzerkonten für Systemadministration und Sachbearbeitung
- Gesicherte Aufbewahrung administrativer Passwörter im Sicherheitsschrank (Tresor)
- Verwaltung der IT-Systeme durch eigene Administratoren
- Sperren der Bildschirme beim Verlassen der Arbeitsplätze durch Funktionstasten
- Automatisches sperren des Arbeitsplatzbildschirms bei Leerlauf bzw. Inaktivität des Rechners
- Ausschließlich passwortgestützte Aufhebung der Bildschirmsperre
- Verschlüsselung von Notebookfestplatten
- Sperrung von USB-Schnittstellen für externe Datenträger
- Sicherung des Netzwerks durch eine Hardwarefirewall und laufende Aktualisierung der Soft- und Firmware

1.3. Zugriffskontrolle

Maßnahmen, die 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 können.
Es existieren bei ODS folgende Maßnahmen zur Zugriffskontrolle:

- Differenziertes Berechtigungskonzept. Schriftliche Festlegung von Zugriffs- und Benutzerberechtigungen für jeden Mitarbeiter je nach Aufgabengebiet.
- Prozess zur Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen ist implementiert.
- Verbot der Verwendung privater bzw. nicht genehmigter Datenträger im internen Netzwerk.
- Sichere Aufbewahrung von mobilen Datenträgern
- Richtlinien zur ordentlichen Entsorgung/Vernichtung von unbrauchbaren bzw. nicht mehr gebrauchten Datenträgern.
- Daten sind grundsätzlich auf den Server, nicht lokal am Arbeitsplatz, gespeichert.
- Regelmäßige und automatische Löschung von nicht mehr benötigten Daten nach Löschungskonzept.

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.
Es existieren folgende Maßnahmen bei ODS zur Trennungskontrolle:

- Kundentrennung: Daten werden in getrennten kunden- und auftragsspezifischen Verzeichnissen gespeichert
- Festgelegte Dateinamenskonvention - Eindeutige Identifizierung eines jeden Auftrags.
- Zweckgebundene Verarbeitung von Daten. Es werden nur solche Daten erhoben, gespeichert und verarbeitet, die unmittelbar dem eigentlichen Zweck dienen.

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden.

- Zurzeit wird bei ODS keine Maßnahme zur Pseudonymisierung angewandt.

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

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogenen Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Es existieren folgende Maßnahmen bei ODS zur Weitergabekontrolle:

- Feststellung befugter Personen
- Verschlüsselung der Daten
- Ausgabe von Datenträgern nur an autorisierte Personen
- Aufbewahrung mobiler Datenträger in Sicherheitsschrank (Tresor) und Bestandskontrolle mobiler Datenträger
- Zugriffsgeschützte Speichermedien des Dateiservers im gesicherten Serverraum bzw. Serverschrank
- Dokumentierte Vernichtung von Datenträgern/Fehldrucken/Fehlkuvertierungen in Sicherheitsbehältern mit der Sicherheitsstufe 3, die von zertifizierter Entsorgungsfirma entsorgt werden
- Verschlüsselter Datentransport (HTTPS, SFTP) nach dem Stand der Technik
- Sperrung von USB-Anschlüssen an Arbeitsstationen.

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten in Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.
Es existieren folgende Maßnahmen bei ODS zur Eingabekontrolle:

- Eingaben sind nur nach explizierter Anmeldung möglich
- Dokumentierte Eingabeberechtigungen
- Verfahrens- und Arbeitsanweisungen sind definiert und stellen eine flankierende Maßnahme dar.

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Es existieren folgende Maßnahmen bei ODS zur Verfügbarkeitskontrolle:

- Regelmäßig aktualisierter Unternehmensnotfallplan
- Unterbrechungsfreie Stromversorgung durch Einsatz von USV-Geräten an Datenserver und Serversystemen.
- Wöchentliches Backup auf Bandmedium. Aufbewahrung der Bänder in Sicherheitsschrank (Tresor)
- Gespiegelter Datenbestand auf örtlich getrennten Serversystemen
- Sicherung des Netzwerks durch Einsatz einer Hardwarefirewall
- Einsatz eines aktuellen Virenscanners der Firma ESET im Netzwerk. Regelmäßige Virenüberprüfung aller angeschlossenen Rechnersysteme. Regelmäßige Updates der Virendefinition und Software.

- Einsatz eines Spamfilters am E-Mailserver und Blockierung von verdächtigen Domains
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Buchstabe c DS-GVO):
  - Bereithalten der Daten auf Dateiserver bei der ODS GmbH
  - Durch das RAID 5 Verfahren werden einzelne Festplatten des Speicherverbunds vor Ausfall geschützt
  - Zusätzlich werden die Daten regelmäßig auf einem zweiten Dateiserver (ebenfalls Raid 5) als Snapshots über den Tag verteilt gespiegelt, so dass die Daten auch in verschiedenen Zuständen zur Verfügung stehen. Hierdurch werden die Daten vor fehlerhaften Veränderung oder unfreiwilliger Löschung geschützt.
  - Auch bildet die Spiegelung auf einen örtlich vom ersten Datenserver getrennten Rücksicherungsspeicher eine zweite Stufe in der Ausfallsicherheit der Daten.
  - Eine weitere Stufe in der Sicherung der Daten stellt eine Gesamtsicherung aller Daten im wöchentlichen Zyklus auf LTO-Bändern dar.
  - Diese Sicherungen werden zugangssicher in einem Tresor, ebenfalls örtlich von den Dateiservern getrennt aufbewahrt.
  - Zur Wiederherstellung verlorener Daten wird die Software „Backup Exec“ verwendet, die auch maßgeblich für die Anlegung der Sicherheitskopien auf den Rücksicherungsspeicher verantwortlich ist. Dieses System ermöglicht es die verlorenen Daten ohne größere Probleme aus verschiedenen zur Verfügung stehenden Datensätzen wiederherzustellen.
  - In wöchentlichen Wiederherstellungstests werden die Sicherungen auf deren Integrität überprüft.

4. Löschung

Alle Daten werden regelmäßig daraufhin überprüft, ob diese zu Löschen sind. Gleiches gilt bei konkreten Löschungsanfragen betroffener Personen. Es findet eine jährliche Regelüberprüfung nach Ablauf der gesetzlich (insbesondere nach Steuer- und Handelsrecht) vorgeschriebenen Aufbewahrungsfristen statt. Die Vernichtung erfolgt gem. DIN 66399, es gilt Schutzklasse 1.

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

Maßnahmen zur Garantie eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten:

Es existieren folgende Maßnahmen bei ODS:
- Führungskräfte und Mitarbeiter werden durch Schulungen regelmäßig auf das Thema sensibilisiert
- Über Neuerungen und Veränderungen werden die Führungskräfte und Mitarbeiter informiert
- Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- Zur Minimierung von Risiken wird eine Datenschutzfolgenabschätzung vorgenommen.
- Interne Audits finden mindestens 1x jährlich statt. Die Ergebnisse und Auswertungen werden protokolliert und weitere Maßnahmen ggf. abgeleitet.
- Praktizierte Datensparsamkeit und –minimierung, dies wird durch das Löschkonzept unterstützt.
- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle.

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Berlin, 18.04.2018

ODS - Office Data Service GmbH

Margit Jahnke
Datenschutzbeauftragte