Technische und Organisatorische Maßnahmen (Art. 32 DSGVO, Sicherheit der Verarbeitung)

Ziel der getroffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stand der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen ein angemessenes Schutzniveau zu gewährleisten.

Dies kann durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art 24 DSGVO, „Privacy –by-Design", Privacy-by-Default) sowie den Einsatz der Pseudonymisierung und Verschlüsslung personenbezogener Daten geschehen.

Dabei gilt es, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sichergestellt wird und bei einem physischen oder technischen Zwischenfall die Verfügbarkeit und der Zugang zu den personenbezogenen Daten rasch wieder hergestellt werden kann.

1. Vertraulichkeit

Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Maßnahmen zur Zutrittskontrolle
Die Firma A&O Fischer GmbH & Co. KG, Maybachstraße 9, 21423 Winsen (Luhe) ist durch eine Einbruchmeldeanlage gemäß VDS Klasse BSG2 gesichert. Das gesamte Firmengelände ist durch einen Zaun gesichert. Alle Räume werden durch Bewegungsmelder gesichert und sind direkt mit der Alarmanlage verbunden, die über eine direkte Leitung zur Einbruchmeldezentrale verfügt. Bei Einbruch wird parallel zu akustischen und visuellen Hinweisen im und am Gebäude ein stiller Alarm an das beauftragte Sicherheitsunternehmen gegeben. Von dort aus werden dann alle weiteren notwendigen Schritte unternommen (u.a. Benachrichtigung der Polizei, Überprüfung vor Ort). Diese Vorgehensweise wird mindestens zweimal im Jahr mittels einer Alarmübung überprüft und protokolliert.

Alle Außentüren sind verschlossen. Ein Zutritt zu den Geschäftsräumen ist nur den zutrittsberechtigten Personen und Dritten nur in Begleitung eines Mitarbeiters möglich. Der Zutritt zu den Datenverarbeitungsanlagen (Serverräumen) ist nur einem begrenzten Mitarbeiterkreis möglich (z.B. Administratoren).

Alle Räume innerhalb des Betriebsgeländes sind in Sicherheitszonen eingeteilt:

- Sicherheitszone 1: Öffentlicher Bereich
- Sicherheitszone 2: Produktion
- Sicherheitszone 3: Serverräume

Die Zugangsberechtigungen zu den einzelnen Sicherheitsbereichen sind im System hinterlegt, über Zutrittskarten bzw. Chips geregelt und unterliegen einer regelmäßigen Prüfung durch den Datenschutz-

bzw. IT-Sicherheitsbeauftragten. Für die Vergabe von Berechtigungen an Mitarbeiter sind die Vorgesetzten zuständig. Die Steuerung der Zutrittsberechtigungen und deren Entzug erfolgt zentral. Die zutrittsberechtigten Personen können mittels Zutrittskarte in das Gebäude gelangen.
Das Zutrittskonzept lässt es zu, den Zutritt für jeden Bereich und jeden Mitarbeiter im Detail zu regeln. Zusätzlich werden alle Zutritte zu den Eingangsbereichen und zur Produktion videoüberwacht.

Für betriebsfremde Personen (z.B. Wartungspersonal, Besucher) bestehen Zutrittsregelungen. Sie sind nur mit Genehmigung, Protokollierung und Aushändigung von Ausweisen zutrittsberechtigt.
Zu den Zutrittsregelungen für Besucher und Wartungspersonal gehören weiter unter anderem die eigene Erfassung in Listen mit Registrierung und die Ausgabe nummerierter Besucherausweise.
Eine Nutzung von Mobiltelefonen und Kameras in den Betriebsgebäuden ist verboten. Die Einhaltung der Zutrittsschutzmaßnahmen wird im Rahmen interner Audits vom Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten regelmäßig überprüft.

Zugangskontrolle

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen personenbezogener Daten verarbeitet oder genutzt werden, nutzten können.

Maßnahmen zur Zugangskontrolle
Alle Server und PC-Arbeitsplätze die zur Verarbeitung personenbezogener Daten genutzt werden, sind in einem eigenständigen Netzwerk zusammengefasst.

Die Laufwerke (CD-ROM oder Diskette) und USB-Anschlüsse an den PC-Arbeitsplätzen im Produktionsbereich und der Datenerfassung sind für die Nutzung durch die Mitarbeiter gesperrt. Die PC-Arbeitsplätze sind zugangsgeschützt. Benutzer können auf gespeicherte Daten nur zugreifen oder Daten nur speichern, sofern sie dafür berechtigt sind.

Zur Anmeldung/Identifizierung im System muss der Benutzer seine User-ID und sein persönliches Passwort eingeben. Die Zugriffsberechtigungen sind in der Policy „Zugangs- und Zugriffsrechte" hinterlegt, wobei der Zugriff auf die DV-Systeme selbst nur durch die besonders dazu berechtigten und autorisierten Personen erfolgen kann. Zugriffe werden protokolliert.

Die persönlichen Passwörter aller Mitarbeiter sind mindestens 8-stellig und müssen den Komplexitätsvoraussetzungen entsprechen (Zeichen aus drei der vier Kategorien müssen enthalten sein: Großbuchstaben; Kleinbuchstaben; Ziffern; andere als alphabetische Zeichen). Die Passwörter sind nur für einen begrenzten Zeitraum gültig (maximal 12 Wochen). Der Passwortwechsel wird erzwungen. Der Mitarbeiter wird einige Tage vor Ablauf der Gültigkeit darauf hingewiesen, dass sein Passwort in x Tagen abläuft und geändert werden muss. Dies kann sofort erfolgen oder spätestens mit Ablauf der angegeben Frist. Nach Ablauf der Gültigkeit ist der Zugang zum Nutzerkonto so lange gesperrt, bis er durch den Administrator wieder freigegeben wird.
Nach mehrmaliger Falscheingabe eines Passwortes wird das Benutzerkonto gesperrt und kann nur durch einen Administrator wieder freigeschaltet werden.

Passwörter sind stets geheim zu halten. Jeder Mitarbeiter wird mit Beginn seiner Tätigkeit auf das Datengeheimnis gemäß BDSG und unter anderem auf das Sozialdatengeheimnis gemäß § 35 SGB I verpflichtet. Die Mitarbeiter nehmen regelmäßig an den Datenschutz- und Informationssicherheitsschulungen des Datenschutzbeauftragten teil. PC-Arbeitsplätze werden beim Verlassen gesperrt (Clear Screen Policy). Mittels zentraler Domain Policies ist festgelegt, dass die Sperre des Arbeitsplatzes nach 5 Minuten der

Inaktivität des Arbeitsplatzes automatisch erfolgt und der Nutzer sich neu anmelden muss. Der Internet-Zugang und das interne Netzwerk (Intranet) sind gegen ungewollte oder gezielte Zugriffe von außen abgeschottet (Firewall) und geschützt (Virenabwehr). Die Übertragungsleitungen sind abgesichert (siehe Punkt Weitergabekontrolle).

Zugriffskontrolle

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

Maßnahmen zur Zugriffskontrolle
Die Zugriffskontrolle zur Hardware (Server, Rechner etc.) erfolgt durch Benutzerkennungen und Passwörter.

Ein Zugriff auf die Server ist nur mit gesonderter Authentifizierung der Benutzer möglich. Eine personenbezogene Authentifizierung erfolgt durch die Zugangskontrolle. Es bestehen beschränkte und maschinell kontrollierte Zugriffsrechte auf Software und Speichermedien durch Benutzerkennungen und Passwörter. Jeder Mitarbeiter erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeit notwendig sind.

Zugriffsschutz ist auch dadurch gegeben, dass die Absicherung der Daten und Datenträger in sicheren, vor einem Zutritt Unbefugter geschützten Räumen gewährleistet ist.

Die datenschutzgerechte Entsorgung nicht mehr benötigter, bzw. verwendeter Datenträger und Informationen sind durch zertifizierte Entsorgungsfachbetriebe gewährleistet.

Netzpläne werden geführt und gepflegt. Das Netzwerk ist von außen nicht erreichbar.

Der Bereich IT/Administration wird im Rahmen interner Audits durch den Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten kontrolliert.

Trennungskontrolle/-gebot

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindung).

Maßnahmen zum Trennungsgebot
Es erfolgt eine getrennte Aufbewahrung des Posteingangs. Kundenspezifische Druckjobs sind angelegt.

Es erfolgt eine getrennte Verarbeitung von Daten. Die Datenverwaltung erfolgt differenziert (Kunde; Projekt). Durch eine logische Datentrennung werden die Kunden sauber voneinander getrennt gehalten. Eine Möglichkeit zur Verwechslung, zur Vermischung oder zur zufälligen Löschung ist ausgeschlossen.

Die Zugriffsberechtigungen sind über Gruppenrichtlinien und Verzeichnisstrukturen geregelt. Es erfolgt eine getrennte Speicherung von verarbeiteten Daten.

Pseudonymisierung und Verschlüsselung

Eine erforderliche, pseudonymisierte und verschlüsselte Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen.

2. Integrität

Eingabekontrolle

Ziel der Eingabekontrolle ist es, das nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen zur Eingabekontrolle
Das Einloggen in das interne Verarbeitungssystem der A&O ist ausschließlich autorisierten Mitarbeitern möglich (revisionssichere Protokollierung in den Logfiles).

Die Authentifizierung der User erfolgt durch Benutzername und Kennwort (siehe Zutrittskontrolle)

Eine digitale Signatur der bearbeiteten Belege im Verarbeitungssystem. Dies gewährleistet die Transparenz und Nachvollziehbarkeit, welcher Mitarbeiter, zu welchem Zeitpunkt, Daten eingegeben, geändert bzw. gelöscht hat

Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, 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 und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen zur Weitergabekontrolle
Eine verschlüsselte Weitergabe personenbezogener Daten ist zwingend vorgesehen. Zumindest durch eine Verschlüsselung der Archivfiles, z. B. ZIP mit starker Verschlüsselung oder einer höheren Verschlüsselungsstufe durch eine PGP-Verschlüsselung oder SMIME. Eingerichtet sind zusätzlich Datenübertragungswege per SFTP oder VPN.

Maßgebend ist die Kundenanforderung im Einzelfall, die ausdrücklich schriftlich erfolgen muss. Der Datenaustausch zwischen den Standorten erfolgt auf sicherem Weg (z.B. VPN; SFTP) Alle Datenübertragungen werden protokolliert.

Bei Dateneingang wird die Datenübertragung auf ihre Vollständigkeit und ihre Richtigkeit hin überprüft.

Es besteht eine differenzierte Datenverwaltung (Kunde; Projekt), um zu gewährleisten, dass die Daten sauber getrennt gehalten werden und damit keine Möglichkeit der Verwechselung, Vermischung oder zufälligen

Löschung besteht.

Die Datenlöschung erfolgt automatisiert 3 Monate nach Auftragende in datenschutzgerechter Form. Die Dreimonatsfrist ist zwingend, es sei denn, eine ausdrückliche schriftliche Kundenanforderung bedingt eine abweichende Handhabung.

Datenträger werden nur an autorisierte Personen und protokoliert übergegeben.

Die Datenträgervernichtung erfolgt kontrolliert, protokolliert und durch einen zugelassenen sowie zertifizierten Vernichtungsdienstleister.

Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen zur Auftragskontrolle
Sämtliche Verträge, Auftragsbestätigungen liegen schriftlich vor und enthalten sämtliche Pflichten, Aufgaben und Vorgaben von Auftraggeber und Auftragnehmer.

Die mit der Auftragsbearbeitung befassten Mitarbeiter werden in die Auftragsspezifikationen des Kunden und den sich daraus ergebenden Verfahrens- und Arbeitsanweisungen eingehend eingewiesen. Es gibt kundenspezifische Verfahrensanweisungen. Die Mitarbeiter werden regelmäßig in den Bereichen von Datenschutz und Informationssicherheit geschult.

Im Rahmen des integrierten Managementsystems werden die Arbeitsergebnisse regelmäßig durch Aufzeichnungen der Produktion, Stichproben durch das QM- und ISMS-Team sowie interne und externe Audits überprüft.

Es besteht ein dokumentiertes Verfahren zur Lieferantenauswahl-, und -bewertung sowie ein spezielles Verfahren zur Lieferanten Auditierung.

3. Verfügbarkeitskontrolle und Belastbarkeit

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen zur Verfügbarkeitskontrolle
Neue IT-Verfahren sowie neue Software müssen freigegeben werden. Ein firmenweiter Virenschutz ist im Einsatz.

Ein Notfallhandbuch/-konzept ist erstellt.

Überprüfungen der Sicherheitsverfahren erfolgen regelmäßig.

Serverräume sind mit Klimaanlage, Feuerlöschgeräten und USV ausgestattet. Es erfolgt eine tägliche Datensicherung der relevanten Bereiche. Die Sicherung der Daten erfolgt gemäß der Vorgaben des „Betriebshandbuch Operating System". Alle wichtigen Hardware/System-Komponenten sind redundant ausgelegt.

Eine Notstromversorgung ist durch einen gesicherten Shut-Down-Prozess gewährleistet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Ziel ist es, die Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen hinsichtlich der Gewährleistung eines angemessenen Schutzniveaus in der Verarbeitung zu prüfen und zu dokumentieren.

Die A&O Fischer GmbH & Co. KG hat ein Informations-Sicherheits-Management-System (ISMS) implementiert und ist nach ISO/IEC 27001/2020 zertifiziert.
Die Zertifikats-ID. lautet: DSC.471.07.2017

Im Rahmen des Zertifizierungsverfahrens erfolgen jährliche Überprüfungsaudits durch die externe Zertifizierungstelle sowie ein Zertifizierungsaudit in 3-jährlichem Rhythmus. Darüber hinaus finden jährliche, sowie bei besonderen Anlässen Interne Audits statt.

Weitere Maßnahmen

Maßnahmen Personal

Einarbeitung neuer Mitarbeiter

Neu eingestellte Mitarbeiter werden innerhalb der ersten Wochen geschult und auf den Datenschutz sowie die Einhaltung der Maßnahmen zur IT- und Informationssicherheit verpflichtet.

Informationssicherheit/ Datenschutz- u. Geheimhaltungsverpflichtung

Nach Einweisung und Schulung sind alle Mitarbeiter verpflichtet, eine Informationssicherheits-/Datenschutz- und Geheimhaltungsverpflichtung zu unterschreiben; dies wird Bestandteil des Arbeitsvertrages. Die Verpflichtung wird in der Personalakte des jeweiligen Mitarbeiters hinterlegt. Konsequenzen aus Pflichtverletzungen werden den Mitarbeitern deutlich gemacht. Eine Abschrift der Datenschutz- und Geheimhaltungsverpflichtungserklärung wird dem Mitarbeiter ausgehändigt.

Regelmäßige Schulungen

Alle Mitarbeiter werden regelmäßig auf den neuesten Stand des Datenschutzes und den Maßnahmen zur Gewährleistung der IT-Sicherheit im Unternehmen gebracht. Weiterhin wird auf Sicherheitslücken hingewiesen und die Mitarbeiter mit den neuen Bestimmungen vertraut gemacht. Die Gesetzestexte zu den datenschutzrechtlichen Bestimmungen werden den Mitarbeitern auf Wunsch zur Verfügung gestellt.

Verfahrensweise beim Ausscheiden von Mitarbeitern

Mitarbeiter die das Unternehmen verlassen, unabhängig vom Grund, werden abschließend mündlich und schriftlich auf den Fortbestand der Geheimhaltungs- und Datenschutzbestimmungen hingewiesen und eventuelle Konsequenzen bei Zuwiderhandlungen dargestellt. Überdies werden beim Ausscheiden eines Mitarbeiters sämtliche Maßnahmen gemäß der Anweisung „Mitarbeitereintritt /-wechsel- und -austritt“ ergriffen.

Maßnahmenbereich Gebäudesicherung

Sichtschutz

Alle Fenster sind mittels Spezialfolien gegen Einsichtnahme Unbefugter gesichert.

Brandschutz

Die Brandschutzverordnung der Feuerwehr wird durch Brandschutzbegehungen überprüft und die hierbei gemachten Auflagen werden umgesetzt. In allen Räumen herrscht Rauchverbot. Alle Räume sind mit einer Brandmeldeanlage ausgestattet.

Allgemeine Sicherungsmaßnahmen

Die Abteilungs- und Teamleiter sind verpflichtet nach Abschluss der Arbeiten auf geschlossene Fenster, Sichern aller Türen etc. zu achten und für die Sicherung des Gebäudes in dem Bereich zu sorgen, in dem ihre Abteilung liegt.

Schlussanmerkung:

Datenschutz unterliegt bei A&O einem ständigen Verbesserungsprozess und wird den jeweils aktuellen Datenschutzbestimmungen angepasst. Wir arbeiten ständig an diesem Thema und aktualisieren auch dieses Dokument immer wieder.