Beschreibung Technische und organisatorische Maßnahmen (TOMs)

der Organisation: HEINE Optotechnik GmbH & Co. KG

Hinweis
Allgemeines Gleichbehandlungsgesetz (AGG) Aus Gründen der leichteren Lesbarkeit wird in diesem Dokument auf eine geschlechterspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.

4.1 Datensicherheit Beschreibung TOMs

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

Inhalt

4.1 Datensicherheit Beschreibung TOMs

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

1 Einleitung

Datensicherheit ist ein wichtiger integrierter Part im Datenschutz. Über Datensicherheit werden die technischen und organisatorischen Maßnahmen geregelt, die erforderlich sind, um den Schutz von personenbezogenen Daten bei automatisierter Verarbeitung, also in Systemen oder Programmen, zu gewährleisten.

Im Fall des Einbezugs von Auftragsverarbeitern müssen diese ebenfalls auf die Einhaltung von Datensicherheit geprüft werden (Art. 28 DSGVO).

Die Europäische Datenschutzgrundverordnung (DSGVO) enthält in Art. 32 Abs. 1 DSGVO Vorgaben darüber, dass personenbezogene Daten über adäquate technische und organisatorische Maßnahmen sicher verarbeitet werden müssen. Die Umsetzung der Schutzziele (= Maßnahmen) bleibt dabei dem Verantwortlichen*, „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen*" (Art. 32 DSGVO) selbst überlassen.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennt die DSGVO verschiedene Kontrollbereiche, die jeweils verschiedene Unterpunkte beinhalten:

(1) Pseudonymisierung und Verschlüsselung wo immer möglich
(2) Vertraulichkeit
(3) Integrität
(4) Verfügbarkeit und Belastbarkeit
(5) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren.

2 Organisatorisches

Die gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus und gibt den Mitarbeitern schriftliche Vorgaben in Form von Arbeitsanweisungen, Richtlinien und Merkblätter für die Einhaltung. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffende Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie entweder in die Verantwortung von Auftragsverarbeitern fallen und daher gesondert geregelt und geprüft werden oder da aus Gründen der Vertraulichkeit nicht alle Details veröffentlicht werden sollen.

3 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der betrieben werden.

3.1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Wo immer möglich, werden personenbezogene Daten ausschließlich pseudonymisiert (also ohne direkte Erkennbarkeit einer betroffenen Person) verarbeitet. Zudem sollten Daten, wo immer möglich, ausschließlich verschlüsselt versendet oder gespeichert werden. Dabei gilt das Prinzip der Verhältnismäßigkeit.

3.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

3.2.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Maßnahmen
Es liegt Beschreibung der gesamten am Standort eingesetzten Zutrittskontrollmaßnahmen vor.
Es handelt sich um umzäuntes Grundstück
Es gibt Sicherungsmaßnahmen gegen Überfälle.
Es existieren angemessene, nicht maschinelle Zutrittskontrollen zu dem Gebäude.
Es besteht eine Pflicht zum Tragen von Dienst- oder Firmenausweisen.
Es besteht eine Kennzeichnungspflicht für fremde Personen durch sichtbar zu tragenden Ausweisen.
Die Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben.
Die Netzwerkkomponenten befinden sich in dafür vorgesehenen zutrittskontrollierten Räumen.

3.2.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Maßnahmen
Für alle Informationssysteme und Dienste gibt es eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.
Es ist sichergestellt, dass Benutzer nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind.
Es ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.
Es gibt ein formales Freigabeverfahren, welche Systeme und Applikationen mit personenbezogenen Daten zu durchlaufen haben, bevor diese Netzwerkzugang bekommen dürfen.

Es ist sichergestellt, dass nur autorisierte Geräte von privaten Personen oder Besuchern logischen Zugang zum Netzwerk der Organisation bekommen.
Das WLAN ist vor unbefugtem Zugang gesichert.
Es gibt Maßnahmen zur Identifikation und Authentisierung von externem Wartungspersonal.
Bei der lokalen Wartung durch Externe ist sichergestellt, dass keine Ausrüstungsgegenstände den DV-Bereich unkontrolliert verlassen können.
Bei der Fernwartung wird die Verbindung von einer Person aufgebaut, welche Mitglied der eigenen Organisation ist.
Der Verbindungsaufbau geschieht von innerhalb des Netzwerks aus.
Die eingerichteten Schutzmaßnahmen der Zugangskontrolle werden regelmäßig einem Test unterzogen, um festzustellen, ob sie noch den gewünschten Schutzzweck erfüllen.

3.2.3 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.

Maßnahmen
Es wird der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms gelebt (Clean Desk Policy).
Es gibt Anweisungen, dass DV-Ausstattung (PC, Laptop, Smartphone etc.), falls unbeaufsichtigt, ausreichend (bspw. durch Abmelden vom System usw.) geschützt ist.
Es gibt Anweisungen, wie mit nicht mehr benötigten Datenträgern (einschließlich beschriebenem oder bedrucktem Papier) umzugehen ist.
Die Daten auf PCs, Laptops werden verschlüsselt.
BitLocker wird eingesetzt, so dass von hinreichend sicheren Verschlüsselungsalgorithmen und Schlüssellängen ausgegangen werden kann.
Die Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind, ist geregelt.
Es ist sichergestellt, dass Dokumente und Datenträger, deren Aufbewahrungsfrist abläuft, nachhaltig vernichtet bzw. gelöscht werden.

3.2.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen

Personenbezogene Daten auf den Systemen werden physisch voneinander getrennt (Verarbeitung unterschiedlicher Datensätze auf getrennten Systemen).
Personenbezogene Daten auf den Systemen werden logisch voneinander getrennt (unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit)).
Die im Unternehmen eingesetzten Systeme sind mandantenfähig.
Die Mandantenfähigkeit für die davon betroffenen Verfahren ist durchgängig realisiert.
Office-, Entwicklungs-, Test- und Wirksysteme befinden sich in klar voneinander getrennten Netzsegmenten, wo möglich sogar physikalisch voneinander getrennt.

3.2.5 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 und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Maßnahmen
Pseudonymisierungsverfahren im Unternehmen werden mit getrennter Aufbewahrung der Zuordnungsdatei eingesetzt.

3.3 Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

3.3.1 Weitergabekontrolle

Maßnahmen, die 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
Alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, sind zur Einhaltung der Vertraulichkeit verpflichtet.
Allen neuen Mitarbeitern werden bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz ausgehändigt.
Die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, werden durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden.
Es gibt einen Prozess für ausscheidende, insbesondere gekündigte Mitarbeiter.
Angemessene Sicherheitsmaßnahmen für den physischen Transport von Datenträgern (inkl. Papier) sind umgesetzt.
Es ist sichergestellt, dass Daten nur an die vom Auftraggeber festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden.

Die Übermittlung von weitergegebenen Daten erfolgt verschlüsselt.
Bei der Weitergabe von Daten wird, soweit möglich, von den Möglichkeiten der Anonymisierung/Pseudonymisierung Gebrauch gemacht.

3.3.2 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.

Maßnahmen
Die protokollierten Daten unterliegen einer strengen Zweckbestimmung.
Die protokollierten Daten sind gegen unbefugte Einsicht oder Manipulation geschützt.

3.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) und c) DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Maßnahmen
Ein Notfallhandbuch existiert und wird laufend aktualisiert.
Die Verantwortlichkeit und Weisungsbefugnis im Katastrophenfall eindeutig geregelt.
Die Systeme sind gegen Ausfall abgesichert.
In regelmäßigen Abständen wird überprüft, ob die Versorgung mit Fernmelde- und Datenleitungen, Strom, Wärme und Wasser noch ausreichend ist.
Die Versorgungsleitungen verlaufen unterirdisch.
Es werden ausreichend dimensionierte USVs eingesetzt.
Die USV ist auf eine Versorgungszeit von 40 Minuten ausgelegt.
Es findet eine ständige Überwachung der Ausgangsspannung(en) statt.
Die USV-Anlage verfügt über Überspannungsschutzeinrichtungen.
Es gibt Blitzschutzeinrichtungen.
Im Serverbereich befinden sich keine brennbaren Gegenstände.

Ein Frühwarnsystem mit automatischen Brandmeldern ist installiert.
Das Brandmeldesystem wird regelmäßig gewartet.
Druckknopfmelder zur manuellen Alarmauslösung sind vorhanden und deutlich gekennzeichnet.
Alarmmeldungen des Frühwarnsystems werden weitergegeben.
Es findet eine regelmäßige Wartung und Überprüfung der Rauchmelder und Handfeuerlöscher statt.
Die Anforderungen an das Backup sind in einem Backup-Konzept dokumentiert.
Es werden regelmäßige Backups durchgeführt.
Die Backups sind verschlüsselt.
Die Backups sind vor Diebstahl und Zerstörung geschützt.
Die Prozesse für die Sicherung wurden erstellt und in Handlungsanweisungen dokumentiert.
Die für die Sicherung verantwortlichen Personen wurden namentlich benannt und dokumentiert.
Es wird regelmäßig getestet, ob das Backup brauchbar ist.
Es gibt für den DV-Wiederanlauf eine schriftliche Unterlage.
Es existiert ein eigener Archivraum.
Es existiert ein Sicherheitsarchiv in einem anderen Gebäude oder Brandabschnitt.
Der Zutritt zum Archiv ist auf einen genau festgelegten Personenkreis eingeschränkt.
Es gibt eine Notabschaltung der Stromversorgung.
Es gibt eine sinnvolle Aufteilung in Brandabschnitte.
Die Einhaltung der Lufttemperatur und -feuchtigkeit wird überwacht.
Es wird Antivirensoftware eingesetzt.
Es wird ein IDS (intrusion detection system) bzw. IPS (intrusion prevention system) eingesetzt.

3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d) DSGVO)

3.5.1 Auftragskontrolle

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

Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf die Wahrung der Vertraulichkeit verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.

Sollte die bei der Datenverarbeitung Auftragsverarbeiter einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Auftragnehmer im Sinne Art. 28 DSGVO und Art. 32 Abs. 1 DSGVO.

Voraussetzungen für das Eingehen einer Auftragsverarbeitung ist grundsätzlich eine rechtliche Grundlage. Für einen Vertrag zur Auftragsdatenverarbeitung nach Art. 28 Abs. 3 DSGVO müssen alle geforderten Maßnahmen und Vorgaben eingehalten werden.

Maßnahmen
Alle Auftragsverarbeiter sind vollständig vertraglich verpflichtet.
Alle Auftragsverarbeitungsverträge sind datenschutzrechtlich geprüft.