| | |
|---|---|
| **1** | **Unternehmen** |
| 1.1. | Benennen Sie Produkte und Dienstleistungen Ihres Unternehmens und erläutern Sie diese stichwortartig. |
| 1.2. | Werden im Unternehmen – außerhalb der Personalabteilung – besondere Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verarbeitet? |
| 1.3. | Verarbeitet das Unternehmen (auch) personenbezogene Daten von Kindern? Falls ja, auf welcher Rechtsgrundlage erfolgt die Verarbeitung? |
| 1.4. | Bitte legen Sie ein aktuelles Organigramm des Unternehmens oder der Unternehmensgruppe vor. |
| 1.5. | Benennen Sie sämtliche Standorte Ihres Unternehmens jeweils mit Angabe der wesentlichen am Standort stattfindenden Datenverarbeitungen (Stichworte). |
| 1.6. | Befinden sich Standorte des Unternehmens außerhalb der EU oder des Europäischen Wirtschaftsraumes („EWR“)? |
| 1.7. | Sofern es Standorte außerhalb der EU oder des EWR gibt, erfolgt mit diesen Standorten ein Austausch von Daten oder eine gemeinsame Nutzung von IT-Ressourcen? |
| 1.8. | Geben Sie die Anzahl der Mitarbeiter Ihres Unternehmens an, bei mehreren Standorten bitte auch pro Standort. Differenzieren Sie nach fest angestellten Mitarbeitern, Auszubildenden, Aushilfen, Praktikanten, Studenten etc. |
| 1.9. | Besteht in Ihrem Unternehmen oder der Unternehmensgruppe ein Betriebsrat? |

| | |
|---|---|
| **2** | **Datenschutzdokumentation** |
| 2.1. | Bitte legen Sie das aktuelle Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) vor. |
| 2.2. | Falls das Verzeichnis von Verarbeitungstätigkeiten unvollständig ist oder nicht existiert, benennen Sie bitte die Abteilungen und Prozesse im Unternehmen, die mit personenbezogenen Daten umgehen. |
| 2.3. | Sofern konzernverbundene Unternehmen mit personenbezogenen Daten des Unternehmens umgehen, legen Sie bitte die entsprechenden Vereinbarungen nach Art. 28 DS-GVO vor oder benennen Sie die Rechtsgrundlage für die Übermittlung. |
| 2.4. | Legen Sie bitte eine Liste aller Dienstleister vor, die für Sie im Rahmen einer Auftragsverarbeitung tätig sind und fügen Sie die abgeschlossenen Verträge zur Auftragsverarbeitung bei. Vermerken Sie bitte – soweit bekannt – jeweils, wenn der Vertrag ganz oder teilweise auf Standardvertragsklauseln (Art. 28 Abs. 7, 8 DS-GVO) beruht, ob sich der Auftragsverarbeiter zur Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) verpflichtet hat und/oder gem. Art. 42 DS-GVO zertifiziert ist. |
| 2.5. | Bitte legen Sie von den Auftragsverarbeitern bereitgestellte Unterlagen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DS-GVO vor. |
| 2.6. | Falls die Liste der Auftragsverarbeiter unvollständig ist oder nicht existiert, übergeben Sie dem Auditor bitte eine Liste der Unternehmen und Dienstleister, die für Sie Datenverarbeitungen vornehmen (inkl. Wartung von Datenverarbeitungsanlagen). |
| 2.7. | Wie wird im Unternehmen sichergestellt, dass die Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur nach Weisung des Verantwortlichen verarbeiten? |
| 2.8. | Verfügt das Unternehmen über ein Datenschutzmanagementsystem und wird dieses aktiv genutzt? |
| 2.9. | Bestehen Zertifizierungen nach Art. 42 DS-GVO? |

| 3 | **Datenschutzorganisation** |
|---|---|
| 3.1. | Besteht ein Prozess für die Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen? |
| 3.2. | Wie ist im Unternehmen sichergestellt, dass die Informationspflichten gegenüber den Betroffenen vollständig und rechtzeitig erfüllt werden? |
| 3.3. | Wer legt die Anforderungen an die technischen und organisatorischen Maßnahmen fest, die externe Dienstleister einzuhalten haben? |
| 3.4. | Existiert ein dokumentierter Prozess zum Umgang mit Auskunftsverlangen nach Art. 15 DS-GVO? Bitte legen Sie die Prozessbeschreibung vor. |
| 3.5. | Wie ist sichergestellt, dass Forderungen Betroffener nach Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten geprüft und umgesetzt werden können? |
| 3.6. | Wie ist die Einhaltung der gesetzlichen Archivierungs- und Löschungsfristen im Unternehmen sichergestellt? |
| 3.7. | Besteht ein Maßnahmenplan für den Fall, dass der Schutz personenbezogener Daten verletzt wird (Art. 33, 34 DS-GVO)? |
| 3.8. | Wie erfolgt die regelmäßige Unterrichtung der Beschäftigten zu Datenschutzthemen? Besteht ein Schulungsplan? |
| 3.9. | Wie ist organisatorisch sichergestellt, dass vor jeder Verarbeitung von personenbezogenen Daten geprüft wird, ob die geplante Verarbeitung zulässig ist? |
| 3.10. | Wie werden im Unternehmen die Grundsätze des „Datenschutz durch Technikgestaltung“ (Privacy-by-design) und der „datenschutzfreundlichen Voreinstellungen“ (Privacy-by-default) umgesetzt? |
| 3.11. | Hat das Unternehmen ein Datenschutzkonzept? Falls ja: Bitte vorlegen. |
| 3.12. | Gibt es im Unternehmen ein aktuelles Rollen- und Rechtekonzept? |

| | |
|---|---|
| 3.13. | Wer legt im Unternehmen fest, welche (Zugriffs-)Rechte Mitarbeiter bei Einstellungen oder Versetzungen erhalten und welche ggf. entzogen werden müssen? |
| 3.14. | Erfolgt die organisatorische Rechtebewilligung getrennt von der technischen Rechteeinräumung? Wie wird dokumentiert, welche Rechte ein User erhält? |
| 3.15. | Besteht ein standardisierter Prozess beim Ausscheiden von Mitarbeitern? |
| 3.16. | Ist die private Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und ggf. weiteren dienstlichen Geräten klar geregelt? Bitte Regelung vorlegen. |
| 3.17. | Wie wird bei einem bestehenden Verbot der privaten Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und weiteren dienstlichen Geräten die Einhaltung des Verbots kontrolliert? |
| 3.18. | Besteht ein Prozess zur Beauftragung externer Dienstleister, die mit personenbezogenen Daten umgehen? Bitte legen Sie eine Prozessbeschreibung vor. |
| 3.19. | Wie wird das Recht auf Datenübertragbarkeit vom Unternehmen sichergestellt? Besteht ein entsprechender Prozess? |
| 3.20. | Sofern personenbezogene Daten öffentlich gemacht wurden: Welche Prozesse sind implementiert, wenn Betroffene ihr Recht auf Vergessenwerden gelten machen? |
| 3.21. | Wie werden Widersprüche Betroffener gegen Datenverarbeitungen auf Grundlage einer Interessenabwägung vom Unternehmen geprüft und umgesetzt? |

| | |
|---|---|
| **4** | **IT-Systeme** |
| 4.1. | Bitte legen Sie eine Übersicht über die IT-Infrastruktur und alle Systeme vor, auf denen personenbezogene Daten verarbeitet werden. |
| 4.2. | Bitte benennen Sie, sofern nicht in 4.1 enthalten, die zentralen Standorte von Datenverarbeitungssystemen und deren Hauptaufgaben. |
| 4.3. | Setzen Sie eine zentrale Unternehmenssoftware (ERP-System) ein? Falls ja, welche? |
| 4.4. | Sofern Sie eine ERP-Software einsetzen, wird diese auf eigenen Systemen (intern oder Housing), auf fremden Systemen (Hosting) oder als SaaS-Lösung betrieben? |
| 4.5. | Nutzt das Unternehmen oder nutzen Mitarbeiter und Abteilungen Cloud-Speicherdienste wie Google Drive, Dropbox oder Microsoft OneDrive? |
| 4.6. | Nutzt das Unternehmen Cloud-Services wie Salesforce (CRM), Datapine (Data Analytics) oder ähnliche Dienste? |
| 4.7. | Werden die Standorte regelmäßig einer externen Prüfung unterzogen (z. B. ISO 27001, IT-Grundschutz, geprüftes Rechenzentrum)? Bitte legen Sie die jeweils aktuellen Prüfberichte vor. |
| 4.8. | Unterziehen Sie Systeme regelmäßigen Sicherheitsüberprüfungen (z. B. Penetration-Tests oder Security Audit Trails)? Bitte legen Sie aktuelle Prüfberichte oder Logs vor. |
| 4.9. | Besteht ein externer Zugriff auf einzelne oder alle Systeme im Netzwerk (z. B. für Home Office, E-Mail-Abruf oder Fernwartung)? Bitte listen Sie auf, welche Nutzergruppen auf welche Systeme Zugriff haben und wie dieser Zugriff abgesichert wird. |
| 4.10. | Können Mitarbeiter auf Ihren Clients, Laptops oder Tablets eigenständig Software installieren? |
| 4.11. | Werden die Festplatten/Speichereinheiten mobiler Geräte verschlüsselt? |
| 4.12. | Setzen Sie ein Mobile Device Management ein? Falls ja, welches? |