Selbstcheck DSGVO

Diese Checkliste soll Ihnen dabei helfen, einen ersten Überblick über die wesentlichen Anforderungen der DSGVO an Ihr Unternehmen zu bekommen. Für eine detaillierte Analyse wenden Sie sich bitte an einen DSGVO-Experten oder besuchen Sie die Serviceangebot der WKO im Internet.

Was sind personenbezogene Daten?

„Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

Welche Daten werden im Unternehmen verarbeitet?

- Werden personenbezogene Daten (z.B.: Name, Geburtsdatum, IP-Adresse usw.) verarbeitet, wenn ja welche?
- Werden besonders schützenswerte Daten verarbeitet (medizinische Daten, Religionszugehörigkeit usw.)
- Werden Informationsdienste auch Kindern angeboten?

Wozu werden die Daten im Unternehmen verarbeitet?

- Welchem Zweck dienen die Datenverarbeitungen?
- Welche rechtlichen Grundlagen gibt es dafür?

Wie werden Daten im Unternehmen verarbeitet?

- Existiert ein Verzeichnis der Datenverarbeitungen? Wenn ja ist es vollständig und wird es regelmäßig gewartet?
- Werden personenbezogene Daten verwendet, um persönliche Aspekte (wie z.B.: Kreditwürdigkeit, Aufenthaltsort) einer Person zu analysieren oder vorherzusagen?
- Bestehen Dokumentationsvorschriften? Wenn ja, werden sie erfüllt?
- Findet die Verarbeitung in einer nachvollziehbaren und transparenten Weise statt?

Vertragsgrundlagen

- Liegen Einwilligungen der betroffenen Personen über die Datenverarbeitung vor?
- Sind alle rechtlichen Texte (AGBs, Impressum, Datenschutzerklärung usw.) an die neuen Anforderungen angepasst?

Umgang mit Betroffenenrechten

- Können Anträge auf Auskunft, Löschung, Berichtigung von personenbezogenen Daten entgegengenommen und erfüllt werden?
- Gibt es eine Stelle im Unternehmen an die sich Betroffene wenden können?
- Können persönliche Daten übertragen werden? (z.B.: Export in lesbarem Format)
- Werden Verletzungen beim Schutz persönlicher Daten im Unternehmen erkannt, dokumentiert und bei kritischen Verletzungen innerhalb von 72 Stunden an die Behörde und die Betroffenen gemeldet?

Findet eine Verarbeitung im Ausland statt?

- Werden Daten mit dem EU-Ausland ausgetauscht? Wenn ja, gibt es eine Rechtsgrundlage dafür?
- Werden Daten mit dem Nicht-EU Ausland ausgetauscht (z.B.: Behörden, Dropbox usw.)

Sind Dritte an der Datenverarbeitung beteiligt?

- Verarbeiten andere Unternehmen („Auftragsverarbeiter") Daten aus Ihrem Unternehmen (z.B.: Lohnverrechnung, Cloud-Computing, Webshop Anbieter usw.)?
- Gibt es schriftliche Vereinbarungen mit den Auftragsverarbeitern?
- Erfüllen die Auftragsverarbeiter die Anforderungen der DSGVO?

Sicherheit der Datenverarbeitung

- Sind die in der DSGVO geforderten technischen Sicherheitsmaßnahmen (Psyeudonymisierung, Verschlüsselung, Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Evaluierung) vorhanden?
- Welche organisatorischen Sicherheitsmaßnahmen (Verhaltensregeln, Abläufe...) sind vorhanden, um den Schutz der persönlichen Daten zu gewährleisten?
- Werden bei technischen Maßnahmen die Regeln „privacy by design" und „privacy by default" durchgängig umgesetzt?

Erweiterte Pflichten

- Wird im Unternehmen ein Datenschutzbeauftragter benötigt?
- Besteht eine Verpflichtung zur Datenschutz-Folgenabschätzung?

Haftungsausschluss