EU-DATENSCHUTZGRUNDVERORDNUNG (EU-DSGVO): DIE ULTIMATIVE COMPLIANCE-CHECKLISTE

Jedes Unternehmen mit Mitarbeitern in der Europäischen Union muss der EU-Datenschutzgrundverordnung (EU-DSGVO), die am 25. Mai 2018 in Kraft tritt, entsprechen. Sie sind sich nicht sicher, ob Ihr Unternehmen den Anforderungen tatsächlich gerecht wird? Die folgende Acht-Punkte-Checkliste hilft Ihrer Personalabteilung, die Anforderungen der neuen Regularien zu erfüllen.

1. Bilden Sie eine Taskforce

Die Sicherung der Compliance gemäß der EU-DSGVO ist eine unternehmensweite Aufgabe. Daher ist es wichtig, eine Arbeitsgruppe zu bilden, in welcher Mitarbeiter aus der HR, der Rechts- und IT-Abteilung, aus dem Security Management und dem Risk Management vertreten sind. Treffen Sie sich regelmäßig und definieren Sie Aufgaben mit entsprechenden Verantwortlichkeiten und Abgabeterminen.

2. Prüfen Sie alle personenbezogenen Daten

Prüfen Sie alle personenbezogenen Daten, die in der Personalabteilung gespeichert werden. Dazu gehören Daten von derzeitigen und früheren Mitarbeitern sowie Daten von Bewerbern und Dritten (z. B. Ehepartnern). Bei der Überprüfung von personenbezogenen Daten müssen Sie sich folgende Fragen stellen:

- ☐ Gibt es für diese Daten eine spezielle Verwendung?
- ☐ Was ist die rechtliche Grundlage für die Anforderung dieser Daten?
- ☐ Wurde die Person über die Be- bzw. Verarbeitung der Daten informiert?
- ☐ Wie oft werden diese Daten auf Richtigkeit geprüft?
- ☐ Brauchen wir diese Daten noch?
- ☐ Wie gehen wir mit der Bereinigung von überflüssigen Daten um?

3. Prüfen Sie, wer auf personenbezogene Daten zugreifen kann

Machen Sie eine Bestandsaufnahme und prüfen Sie intern wie extern, wer Zugriff auf personenbezogene Daten hat. Dann stellen Sie fest, wie personenbezogene Daten gesichert werden, insbesondere beim Datentransfer über Landesgrenzen hinweg.

Stellen Sie **bei Mitarbeitern** sicher,

- ☐ dass die richtigen Einzelpersonen und Rollen über die korrekten Zugriffsrechte verfügen.
- ☐ dass ein Prozess definiert ist, um Zugriffsrechte bei Rollenänderungen zu aktualisieren.

Stellen Sie **bei Dritten** sicher,

- ☐ welche juristische Person auf personenbezogene Daten zugreifen muss.
- ☐ wie die juristische Person die personenbezogenen Daten nutzen möchte.
- ☐ ob die Vorgehensweise den Vorgaben der EU-DSGVO entspricht.
- ☐ welche Methoden angewandt werden, um personenbezogene Daten zu schützen.

4. Aktualisieren Sie Ihre Datenschutzrichtlinien

Die EU-DSGVO kann sich auf Ihre bestehenden Datenschutzrichtlinien und Prozesse auswirken. Bei einer Prüfung stellen Sie sicher, dass

- ☐ Sie **Einzelpersonen informieren**, wie ihre Daten genutzt werden, insbesondere wenn es vom Arbeitsrecht vorgeschrieben wird.
- ☐ eine adäquate **rechtliche Grundlage** für die Verarbeitung der personenbezogenen Daten dokumentiert wird.
- ☐ Sie technische und organisatorische Maßnahmen beschreiben, um die **Datensicherheit zu gewährleisten**.

5. Dokumentieren Sie die Handhabung von Anfragen nach personenbezogenen Daten

Die EU-DSGVO gibt Einzelpersonen bestimmte Rechte, wenn es um die Nutzung ihrer Daten geht. Um diese Rechte zu garantieren, müssen Sie folgendes berücksichtigen:

- ☐ Wie gewähren Sie Einzelpersonen den Zugriff auf ihre Daten?
- ☐ Wie beantworten Sie Anfragen zur Korrektur personenbezogener Daten?
- ☐ Unter welchen Bedingungen können personenbezogene Daten auf Anfrage gelöscht werden?
- ☐ Unter welchen Bedingungen können Einzelpersonen ihre Zustimmung für die Verarbeitung ihrer Daten geben oder entziehen?

6. Beschreiben Sie die Vorgehensweise im Falle einer Datenpanne oder -verletzung

Sollte es Fehler beim Umgang mit personenbezogenen Daten gegeben haben, muss die Verletzung innerhalb von 72 Stunden der Datenschutzbehörde gemeldet werden. Ebenso muss die Einzelperson unverzüglich informiert werden. Deshalb ist es wichtig, einen festen Prozess für den Umgang mit Datenpannen und -verletzungen zu haben. Stellen Sie sicher, dass

- ☐ Sie Verantwortlichkeiten definieren für die Untersuchung, Erfassung und Meldung von Datenpannen und -verletzungen.
- ☐ alle Datenpannen und -verletzungen mit sämtlichen Details, Auswirkungen und Maßnahmen dokumentiert werden, um die jeweilige Datenpanne oder -verletzung wieder zu beheben.
- ☐ Sie die Vorgehensweise Ihrer Lieferanten im Falle einer Datenpanne oder -verletzung verstehen.

7. Ernennen Sie einen Datenschutzbeauftragten

Wenn Ihr Unternehmen im Rahmen der Geschäftstätigkeit personenbezogene Daten – als Teil Ihres Produktes oder Ihrer Dienstleistung - verarbeitet, müssen Sie einen Datenschutzbeauftragten ernennen. Er ist für die Einhaltung der Compliance im Rahmen der EU-DSGVO verantwortlich und muss den Schutz der personenbezogenen Daten sicherstellen. Sollte dies zutreffen, ernennen Sie entweder jemanden aus Ihrem Team oder beauftragen Sie einen externen Experten.

8. Informieren und schulen Sie Ihre Mitarbeiter

Die Einhaltung der Compliance im Rahmen der EU-DSGVO erfordert die Mitarbeit von allen Mitarbeitern. Stellen Sie sicher, dass jeder die neuesten Compliance-Regularien kennt und weiß, wer im Falle einer Nichteinhaltung zu informieren ist. Binden Sie das Thema Compliance in jedes Onboarding-Training mit ein. Planen Sie einmal im Jahr eine Schulung für alle Mitarbeiter.