DSGVO

FACTSHEET

März 2019

karriere.at

INHALT

Wir legen großen Wert auf geschlechtliche Gleichberechtigung. Aufgrund der Lesbarkeit der Texte wird bei Bedarf nur eine Geschlechtsform gewählt. Dies impliziert keine Benachteiligung des jeweils anderen Geschlechts. Trotz sorgfältiger Bearbeitung erfolgen alle Angaben ohne Gewähr und eine Haftung der karriere.at GmbH ist ausgeschlossen. Bitte erkundigen Sie sich jedenfalls bei einem Experten Ihres Vertrauens über die individuellen Maßnahmen für Ihr Unternehmen.

WAS IST DIE DSGVO?

Die neue Datenschutz-Grundverordnung (DSGVO) der EU definiert den Umgang mit personenbezogenen Daten. Darin wird etwa auch geregelt, unter welchen Voraussetzungen Unternehmen Daten verarbeiten dürfen.

Wesentlich ist dabei der Faktor Eigenverantwortung:
Unternehmen müssen anstatt der bislang gängigen Praxis der Vorab-Meldungen (DVR) und der Genehmigung selbst für die Umsetzung der neuen DSGVO-Richtlinien im Unternehmen sorgen. Es müssen also nicht mehr alle Datenanwendungen der Datenschutzbehörde vorab gemeldet werden, sondern diese führt so genannte ex-post Kontrollen durch. Verstöße können mit hohen Strafen geahndet werden.

SEIT WANN IST DIE NEUE REGELUNG GÜLTIG?

Die DSGVO der EU ist mit dem 25. Mai 2018 in Kraft getreten. In Österreich wird die DSVGO durch das Datenschutzanpassungsgesetz 2018 (DSG 2018) umgesetzt, unter anderem auch deshalb, weil die Nationalstaaten innerhalb der EU zu definierten Punkten ergänzende Regelungen treffen können.

Das DSG 2018 ist neben der DSGVO gültig.

WELCHE UNTERNEHMEN SIND VON DER DSGVO BETROFFEN?

Die DSGVO ist in allen Mitgliedsstaaten der EU in Kraft getreten und ist daher auch von allen Unternehmen gleichermaßen umzusetzen. Die Größe des Unternehmens spielt dabei keine Rolle.

Betroffen sind alle Unternehmen, die in irgendeiner Form personenbezogene Daten verarbeiten bzw. damit im Rahmen ihrer Geschäftstätigkeit in Kontakt kommen. Darunter fallen mitunter auch Tätigkeiten wie Datenerhebung, Speicherung, Änderungen, Abfragen, Datenauswertung usw.

In die Regelung fallen auch Unternehmen aus dem EU-Raum, die Informationen zu Kunden aus Nicht-EU-Ländern verarbeiten. Darüber hinaus gilt die DSGVO auch für Unternehmen mit Sitz außerhalb der EU, die mit Daten von EU-Bürgern arbeiten.

WAS SIND PERSONENBEZOGENE DATEN?

Unter personenbezogenen Daten verstehen sich alle Informationen zu einer natürlichen Person. Als personenbezogene Daten gelten auch Informationen, die in Kombination mit anderen Informationen eine Person identifizierbar machen.

Beispiele:
Name, Geburtsdatum und -ort, Wohnadresse, Arbeitsplatz, Ausbildung, Weiterbildung, IP-Adresse, Hobbys, Familienstand etc.

WAS MÜSSEN UNTERNEHMEN SEIT 25. MAI 2018 GEWÄHRLEISTEN?

- **Verzeichnis von Verarbeitungstätigkeiten**
  Dieses tritt an die Stelle der bisher erforderlichen DVR-Meldungen. In dem Verzeichnis müssen die Namen des Verantwortlichen inkl. Kontaktdaten angeführt werden sowie der Zweck der Datenverarbeitung. Ebenfalls müssen die verarbeiteten personenbezogenen Daten, die betroffenen Personen (Kategorien), Empfänger (Kategorien) und gesetzte Maßnahmen zur Datensicherheit aufgelistet werden.

- **Privacy by design / Privacy by default**
  Die verwendete Technik, aber auch die organisatorischen Abläufe zur Datenverarbeitung müssen den Regelungen der DSGVO entsprechen. Darunter fallen auch die vom Unternehmen gesetzten Voreinstellungen (Default), die ebenfalls die Rechte der betroffenen Personen im Sinne des Datenschutzes gewährleisten müssen:
  Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für den konkreten Verarbeitungszweck notwendig sind.

- **Datenschutzbeauftragter**
  Unternehmen, die in ihrem Kerngeschäft regelmäßig und systematisch Daten zur Überwachung betroffener Personen verarbeiten oder sensible Daten verarbeiten, müssen laut DSGVO einen eigenen Datenschutzbeauftragten ernennen.
  Der Datenschutzbeauftragte berät das Unternehmen und kontrolliert die Einhaltung der DSGVO. Die Verantwortung und Haftung liegt allerdings weiterhin beim datenverarbeitenden Unternehmen.

- **Informationspflicht**
  Bereits zum Zeitpunkt der Erhebung der Daten sind die Betroffenen über die Art und Weise der Verwendung und die Betroffenenrechte zu informieren. Informationen wie Kontaktdaten, Verarbeitungszweck, Empfänger, Speicherdauer oder auch Widerrufsrecht müssen den Betroffenen hier zur Verfügung gestellt werden.

- **Datenschutz-Folgenabschätzung**
  Unternehmen, deren Tätigkeit ein „hohes Risiko“ für Betroffene bedeutet, insbesondere die automatisierte Verarbeitung einschließlich Profiling und die Verarbeitung sensibler Daten, sind zu einer Datenschutz-Folgenabschätzung verpflichtet. Das kann insbesondere IT- und Onlineunternehmen durch die Verwendung „neuer Technologien“ betreffen. In dieser Folgenabschätzung müssen sowohl die konkreten Prozesse der Datenverarbeitung beschrieben werden als auch dargelegt werden, warum die verarbeiteten Daten notwendig bzw. verhältnismäßig sind. Auch muss das Risiko für betroffene Personen beschrieben werden und mögliche Abhilfeprozesse im Unternehmen angeführt sein.

- **Meldepflicht**
  Kommt es trotz aller Maßnahmen zu einer Verletzung der Datenschutzbestimmungen, etwa durch einen Hackerangriff oder den Verlust von Daten(trägern), müssen sowohl Datenschutzbehörde als auch die betroffenen Personen innerhalb von drei Tagen (72 Stunden) informiert werden. Stellt jedoch der konkrete Fall voraussichtlich kein Risiko für die Betroffenen dar, entfällt diese Pflicht.

- **Speicherbegrenzung und Fristen**
  Unternehmen, deren Tätigkeit ein „hohes Risiko" für Betroffene bedeutet, insbesondere die automatisierte Verarbeitung einschließlich Profiling und die Verarbeitung sensibler Daten, sind zu einer Datenschutz-Folgenabschätzung verpflichtet. Das kann insbesondere IT- und Onlineunternehmen durch die Verwendung „neuer Technologien" betreffen. In dieser Folgenabschätzung müssen sowohl die konkreten Prozesse der Datenverarbeitung beschrieben werden als auch dargelegt werden, warum die verarbeiteten Daten notwendig bzw. verhältnismäßig sind. Auch muss das Risiko für betroffene Personen beschrieben werden und mögliche Abhilfeprozesse im Unternehmen angeführt sein.

CHECKLISTE: WANN IST ES ERLAUBT, DATEN ZU VERARBEITEN?

- **Einwilligung**
  Der Betroffene muss seine ausdrückliche Einwilligung dazu gegeben haben und der Prozess der Datenverarbeitung entspricht der DSGVO. Das gilt u.a. für die Verarbeitung von Dokumenten (z.B. Lebenslauf) im Zuge einer Bewerbung als auch z.B. der Kommunikation mit dem Kandidaten selbst.

  Die Einwilligungserklärung muss in klarer, einfacher Sprache formuliert sein, freiwillig abgegeben werden und vom Unternehmen jederzeit nachgewiesen werden können. Dazu muss der Betroffene umfassende Informationen über die verarbeiteten Daten, den Zweck der Verarbeitung, Art der Kontaktaufnahme und, wenn vorhanden, dritte Datenempfänger erhalten. Nicht fehlen darf die Information, dass die Einwilligung jederzeit widerrufen werden darf. Auch die Speicherdauer und die Löschfrist der Daten muss Teil der jeweiligen Erklärung sein.

- **Vertragserfüllung**
  Die Daten sind notwendig, um einen Vertrag mit einem Betroffenen zu erfüllen.

- **Gesetzliche Ermächtigung/gesetzliche Verpflichtung**
  Es kann auch sein, dass die Datenverarbeitung vom Gesetzgeber vorgeschrieben ist.

- **Berechtigte Interessen**
  Der Datenverarbeiter bzw. -verantwortliche (z.B. ein Unternehmen) muss berechtigte Interessen an der Verarbeitung der Daten haben und eine Interessensabschätzung für jede Form der Verarbeitung vornehmen.

WIE STEHT ES UM DIE RECHTE DER BETROFFENEN – ALSO DER PERSONEN, DEREN DATEN VERARBEITET WERDEN?

Die DSGVO sieht u.a. folgende Rechte für Betroffene vor.
Anfragen von Betroffenen dazu müssen innerhalb eines Monats unentgeltlich vom Datenverarbeiter bzw. Verantwortliche beantwortet werden.

- **Recht auf Auskunft**
  Jeder Betroffene hat jederzeit das Recht, sich über die „Hard Facts" der Datenverarbeitung zu informieren (z.B. Datenkategorien, Speicherdauer, Herkunft der Daten). Die Auskunftspflicht gegenüber den Betroffenen trifft grundsätzlich den Verantwortlichen. Für Auftragsverarbeiter, die Teil des Prozesses der Datenerhebung bzw. -verarbeitung sind, gilt diese Pflicht nicht (z.B. im Falle einer irrtümlichen Auskunftsanfrage). Es gilt jedoch eine Unterstützungspflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen im Zuge einer Anfrage.
- **Recht auf Berichtigung**
  Ändern sich Daten oder sind diese falsch bzw. unvollständig abgespeichert, können Betroffene verlangen, dass diese berichtigt werden.
- **Recht auf Datenübertragbarkeit**
  Dieses Recht soll den Betroffenen ermöglichen, dass sie „ihre" Daten für andere Zwecke bzw. den privaten Gebrauch wieder verwenden können. In diesem Fall sind nicht nur die Daten bereitzustellen, welche sich direkt auf die Betroffenen beziehen, sondern auch Daten von anderen Personen, wenn diese Daten in enger Verbindung mit den Betroffenen stehen (z.B. Mails, Chatverlauf, Protokolle).
- **Recht auf Widerspruch**
  Das Recht auf Widerspruch besteht nur dann, wenn die Daten des Betroffenen in Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Wahrung berechtigter Interessen des Auftraggebers verarbeitet werden. Der Betroffene muss seinen Widerspruch darauf stützen, dass Gründe vorliegen, die sich aus seiner besonderen Situation ergeben, welche gegen eine Verarbeitung seiner Daten sprechen.

  Der Auftraggeber kann den Widerspruch ablehnen, wenn er nachweist, dass zwingende, schutzwürdige Gründe für die Verarbeitung vorliegen, welche die Interessen, Rechte und Freiheiten des Betroffenen überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Für Fälle des Direktmarketings und Profilings, soweit es mit Direktmarketing in Zusammenhang steht, sieht Art. 21 Abs. 2 DSGVO ein absolutes Widerspruchsrecht vor.

Recht auf Löschung

Betroffene haben darüber hinaus auch das so genannte „Recht auf Vergessen-werden“. Das bedeutet, dass diese die Löschung ihrer Daten beantragen können, wenn diese nicht mehr erforderlich sind oder die Einwilligung zur Datenverarbeitung widerrufen worden ist. Natürlich gilt dieses Recht auch, wenn Daten gesetzeswidrig verarbeitet werden.

ACHTUNG

Eine Löschung muss in allen Systemen durchgeführt werden, also etwa auch in Backups und ausgelagerten Servern. Sind Daten weitergegeben worden (z.B. von einem Personaldienstleister an einen Unternehmenskunden), so muss auch der Empfänger der Daten von dem Löschungsbegehren informiert werden.

DÜRFEN DATEN WEITERGEGEBEN WERDEN?

Ob und unter welchen Voraussetzungen Daten an Dritte weitergegeben werden dürfen, hängt davon ab, was der Empfänger der Daten damit macht:

Verwendet der Empfänger der Daten für eigene Zwecke – etwa für einen Newsletter an potenzielle Neukunden – muss eine Rechtsgrundlage für die Weitergabe bestehen. Die Voraussetzungen sind dieselben wie oben erwähnt:

Checkliste: Wann ist es erlaubt, Daten zu verarbeiten?

Geschieht die Datenverarbeitung durch den Empfänger im Auftrag eines Dritten, genügt es, wenn ein schriftlicher Vertrag geschlossen wird, in denen die Verarbeitungsschritte beschrieben und gegenseitige Rechte bzw. Pflichten festgehalten werden.

WELCHE STRAFEN DROHEN BEI EINEM VERSTOSS GEGEN DIE DSGVO?

Verstöße können mit Geldbußen von bis zu € 20.000.000,– geahndet werden. Handelt es sich um ein Unternehmen, kann die Strafe auch bis zu 4 Prozent des weltweit erwirtschafteten Jahresumsatzes betragen.

WEITERFÜHRENDE LINKS

WKO
EU Datenschutz-Grundverordnung (DSGVO): Checkliste

DATENSCHUTZBEHÖRDE
Datenschutz-Grundverordnung

RECHTSANWALTSPARTNERSCHAFT BLÜMKE & SCHÖPPL
DS-GVO Checkliste

WKO
EU-Datenschutz-Grundverordnung (DSGVO):
Datenschutzerklärung für Mitarbeiter

KARRIERE.AT
Datenschutz-Grundverordnung: Das müssen Arbeitgeber wissen

ÜBER KARRIERE.AT

karriere.at ist Österreichs größtes Karriereportal. Die Möglichkeiten des Marktführers im Online Recruiting verbinden passende Kandidat*innen mit den besten Arbeitgeber*innen. Durch einen einzigartigen Produktmix finden Unternehmen auf karriere.at passende Kandidat*innen, die eingestellt werden. Stelleninserate auf karriere.at erreichen tausende Jobsuchende und decken den individuellen Recruitingbedarf einfach und bequem ab. Für Arbeitgeber*innen wird der Pool passender Kandidat*innen durch gezielte Vorschläge aus der Bewerberdatenbank zusätzlich erweitert. Die Employer Branding Lösung von karriere.at spricht darüber hinaus potenzielle Mitarbeiter*innen an, die optimal zum Unternehmen passen, denn eine starke Arbeitgebermarke ist wesentlich für den Erfolg im Recruiting.
karriere.at hat sich seit 2005 als eigentümergeführtes Unternehmen zu Österreichs reichweitenstärkstem Karriereportal mit bis zu 4,9 Mio. Besuchen monatlich (Google Analytics 1/2019) und rund 200 Mitarbeiter*innen entwickelt. 97 Prozent Servicezufriedenheit der karriere.at-Kund*innen bestätigen den damit verbundenen, hohen Grad an Kund*innenorientierung.

karriere.at GmbH
Donaupromenade 1, 4020 Linz | +43 (0) 732 90 82 00-0
www.karriere.at | redaktion@karriere.at