Datenschutz-Grundverordnung
Ein Überblick über die wichtigsten Neuerungen und Tipps für die Praxis

Autorin
Katharina Körber-Risak
Rechtsanwältin und Arbeitsrechtsexpertin,
KÖRBER-RISAK Rechtsanwalts GmbH

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in Kraft. Sie bringt EU-weit gravierende Änderungen für Unternehmen bei der Verarbeitung personenbezogener Daten. Das betrifft die Unternehmen auch in ihrer Funktion als Arbeitgeber. Welche datenschutzrelevanten Änderungen mit der DSGVO auf Arbeitgeber zukommen, zeigt der folgende Beitrag.

Die Datenschutz-Grundverordnung (DSGVO) löst die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ab. Sie regelt ab 25. Mai 2018 EU-weit die Verarbeitung personenbezogener Daten. Ein eigenes Arbeitnehmerdatenschutzgesetz ist in Österreich nicht in Sicht und wird derzeit auch nicht gefordert. Stattdessen tritt zum 25. Mai 2018 eine Novelle des Datenschutzgesetzes 2000 („DSG neu") in Kraft. Das bedeutet indes nicht, dass arbeitsrechtlich alles beim Alten bleibt. Sehr umfangreiche Verpflichtungen und eine völlig neue Rechtslage machen die Umsetzung der neuen Regelungen für die Verarbeitung personenbezogener Daten für Arbeitgeber nicht leicht.

Nach der Terminologie der Datenschutz-Grundverordnung sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Datenbegriff ist allumfassend, das heißt, er kann sich auf alle Informationen beziehen, die eine natürliche Person betreffen – vom Namen über Alter, Adresse, Familienstand, politische Gesinnung und Gesundheitszustand bis zur Schuhgröße. Der Begriff „identifizierbar" wird in diesem Zusammenhang sehr weit gefasst, denn auch Online-Kennungen, Standortdaten und besondere Merkmale einer Person wie beispielsweise auffällige Narben gehören zu den fraglichen Informationen. Betroffen ist jede „Verarbeitung", wozu bereits das Erfassen oder Erheben von Daten gehört.

Unternehmen sind ab Inkrafttreten der DSGVO bei der Verarbeitung von personenbezogenen Daten ihrer Arbeitnehmer, aber zum Beispiel auch ihrer Kunden und Lieferanten an die Bestimmungen der Verordnung gebunden. Aus Artikel 5 DSGVO lassen sich folgende Grundsätze ableiten, die generell im Umgang mit Daten berücksichtigt werden müssen:

- **„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz":** Personengebundene Daten dürfen nur verarbeitet werden, soweit es zulässig ist,

und es muss für den Betroffenen nachvollziehbar sein, wie dies geschieht.

- **„Zweckbindung":** Es muss klar sein, wofür die Daten erhoben und verarbeitet werden, und die Daten dürfen nur für diese Zwecke verwendet werden.

- **„Datenminimierung":** Es dürfen nur so viele Daten erhoben werden, wie für den festgelegten Zweck unbedingt notwendig ist.

- **„Richtigkeit":** Die Daten müssen immer auf dem aktuellen Stand gehalten werden. Falsche oder nicht mehr benötigte Daten müssen unverzüglich gelöscht oder berichtigt werden.

Wann ist die Verarbeitung personenbezogener Daten zulässig?

Die Verarbeitung von personenbezogenen Daten ist nach Artikel 6 DSGVO nur dann zulässig, wenn zumindest eine der folgenden Voraussetzungen erfüllt ist:

a. Der Arbeitnehmer hat eine ausdrückliche, jederzeit widerrufbare Zustimmung zur Verarbeitung der Daten erteilt.

b. Die Verarbeitung ist notwendig, um einen (Arbeits-)Vertrag anzubahnen oder zu erfüllen und geschieht auf Initiative des Arbeitnehmers, das heißt, der Arbeitnehmer schickt beispielsweise seine Bewerbung ein. Nicht umfasst sind Daten, die der Arbeitgeber über Personen erhebt, für die er sich interessiert, die sich aber nicht aktiv beworben haben.

c. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung des Arbeitgebers notwendig. Das ist insbesondere im Steuer- und Sozialversicherungsrecht der Fall: Der Arbeitgeber benötigt die Sozialversicherungsnummer des Arbeitnehmers zum Beispiel, um für diesen ein Beitragskonto bei der Sozialversicherung anzulegen und Lohnsteuer abzuführen.

d. Die Verarbeitung ist aus lebenswichtigen Interessen des Arbeitnehmers oder eines Dritten notwendig. Wenn beispielsweise ein Arbeitnehmer am Arbeitsplatz zusammenbricht, kann es notwendig sein, dass der Arbeitgeber Daten über die Blutgruppe und mögliche Impfungen des Mitarbeiters erhebt und weitergibt, die er von Dritten bekommen hat oder Papieren des Arbeitnehmers entnimmt, die dieser bei sich trägt.

e. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Arbeitgebers oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Ein „überwiegendes Interesse" des Arbeitgebers wird beispielsweise bei einem Vertriebsmitarbeiter darin bestehen, dessen Kontaktdaten an potenzielle Kunden weiterzugeben oder diese auf der Homepage zu veröffentlichen. Allgemein anerkannte Betriebszwecke werden bei Daten, die nicht unter die besonderen Kategorien des Artikel 9 DSGVO fallen („sensible Daten"), in der Regel zu einem höheren Interesse des Arbeitgebers führen. Im Detail kann die Beurteilung jedoch schwierig sein. Je weiter die Verarbeitung vom eigentlichen Unternehmenszweck entfernt liegt, desto eher wird das höherwertige Interesse des Arbeitnehmers durchdringen. Verfolgt das Unternehmen etwa den Aufbau einer konzernweiten Datenbank zum Zwecke des Recruitings, dürften die Arbeitnehmerinteressen als vorrangig angesehen werden und es muss eine Zustimmung eingeholt werden.

Die Verarbeitung sensibler Daten

Die Verarbeitung sensibler Daten ist nach Artikel 9 Absatz 2 DSGVO nur in wenigen Ausnahmefällen zulässig. Sensibel sind Daten, aus denen sich die ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit einer Person ergeben. Außerdem zählen dazu genetische und/oder biometrische Daten zur Identifizierung einer Person, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Diese Daten dürfen nur in bestimmten Fällen verarbeitet werden. Für Arbeitsverhältnisse sind zwei Ausnahmen von besonderer Bedeutung:

a. Die Verarbeitung der sensiblen Daten ist aufgrund arbeits- und sozialrechtlicher Schutzvorschriften notwendig. Darunter können auch Gesundheitsvorsorge und Arbeitsmedizin fallen, wobei dann jedoch eine Verarbeitung durch Fachpersonal, in der Regel Ärzte oder Psychologen, erforderlich ist.

b. Die betroffene Person hat die Daten selbst veröffentlicht, zum Beispiel auf einem öffentlich zugänglichen Social-Media-Profil.

Zustimmung des Arbeitnehmers zur Verwendung seiner Daten

Innerhalb eines Unternehmens werden ein und dieselben Daten oft auf unterschiedlichste Art und Weise verarbeitet. Sie tauchen beispielsweise in internen Verzeichnissen auf, werden an die Payroll-Provider oder an Kunden weitergeleitet oder auf der Homepage veröffentlicht. Die Vielzahl der Verwendungsarten macht eine umfangreiche Zustimmungserklärung des Arbeitnehmers aus praktischer Sicht unerlässlich. Liegt diese nicht vor, ist bei jeder einzelnen Datenverarbeitung zu prüfen, ob diese zulässig ist. Um die Zustimmungserklärung gestalten zu können, empfiehlt es sich, im Rahmen eines Datenschutzaudits zu erheben, welche Arbeitnehmerdatenverarbeitungen im Unternehmen regelmäßig anfallen.

Dabei sollten Arbeitgeber auch den in der DSGVO normierten Grundsatz der Datenminimierung im Auge behalten, das heißt überprüfen, ob alle verarbeiteten Daten wirklich notwendig sind und – wenn ja – zu welchem Zweck genau. Danach sollten sie die Zustimmungserklärungen in Angriff nehmen, da pauschale Formulierungen, wie sie bisher üblich waren, nach der DSGVO nicht mehr ausreichend sind. In einer Zustimmungserklärung müssen Unternehmen die Datenanwendung möglichst genau beschreiben, aber auch im Sinne der Transparenz möglichst verständlich formulieren. Der zustimmende Mitarbeiter muss die Folgen seiner Zustimmung abschätzen können, das heißt, ihm müssen die Konsequenzen, aber auch die Widerruflichkeit seiner Erklärung klar sein. Sollte das nicht der Fall sein, ist die Erklärung unwirksam.

Arbeitnehmer können ihre Zustimmungserklärungen jederzeit widerrufen. Dies führt dazu, dass ab dem Zeitpunkt des Widerrufs jede einzelne Datenverarbeitung nach den oben genannten Kriterien überprüft werden

muss und allenfalls unzulässig sein kann. Fraglich ist, ob Arbeitgeber zum Beispiel berechtigt sind, einem Arbeitnehmer zu kündigen, wenn gewisse Datenverarbeitungen ohne dessen Zustimmung unzulässig sind, dies aber eine sinnvolle Tätigkeit des Arbeitnehmers unmöglich macht. Das wäre zum Beispiel dann der Fall, wenn eine Schauspielerin die Zustimmung zur Verarbeitung von Daten zu ihren Körpermaßen widerruft, was die Herstellung von Kostümen für eine Produktion unmöglich macht. Auch ein Außendienstmitarbeiter, der keine Zustimmung erteilt, seine berufliche Mobilnummer weiterzugeben, blockiert damit seine eigene Arbeit, da er für Kunden und den Arbeitgeber unerreichbar ist. In einem solchen Fall ist zu prüfen, ob ein berechtigtes Arbeitgeberinteresse an der Datenverarbeitung besteht, so dass diese auch ohne Zustimmung möglich ist. Ist dies nicht der Fall, verhindert aber der Arbeitnehmer weiterhin seine eigene Vertragserfüllung, könnte dies eine Kündigung aus personenbezogenen Gründen rechtfertigen.

Verarbeitungsverzeichnis statt DVR-Meldepflicht

Bislang mussten Arbeitgeber als „Auftraggeber" von Datenanwendungen eine Meldung beim Datenverarbeitungsregister (DVR) machen. Dabei war jegliches Verarbeiten von Daten zu melden. Diese Form der externen Kontrolle entfällt ab dem 25. Mai 2018. Wo bislang Formalismen und lange Bearbeitungszeiten vorherrschten, wird nunmehr ein völlig neues System eingerichtet. Die Unternehmen werden zur Selbstverwaltung der Daten verpflichtet. Sie werden von der Aufsichtsbehörde kontrolliert und müssen bei Verstößen mit sehr hohen Strafen rechnen. Die Strafandrohungen von bis zu zwanzig Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes eines Unternehmens sind drastisch und können Unternehmen empfindlich treffen.

Um die Verarbeitung von personenbezogenen Daten zu dokumentieren, muss jedes Unternehmen mit mehr als 250 Arbeitnehmern ein „Verzeichnis von Verarbeitungstätigkeiten" führen. Unternehmen mit weniger Mitarbeitern müssen ein solches Verzeichnis führen, wenn sie

- Daten mit besonderem Risiko (etwa Daten von Minderjährigen, große Datenmengen, Daten, die von einem Berufsgeheimnis betroffen sind, etc.),
- Daten nicht nur gelegentlich oder
- sensible Daten

verarbeiten. Diese Voraussetzungen beziehen sich jedoch nicht nur auf personenbezogene Daten von Arbeitnehmern, sondern auch auf die Daten von Kunden oder Lieferanten. Völlig unklar ist daher, was in diesem Zusammenhang eine „nicht nur gelegentliche" Datenverarbeitung sein soll. Bei den meisten Unternehmen ist davon auszugehen, dass Daten von Kunden, Lieferanten und Arbeitnehmern laufend und nicht nur gelegentlich verarbeitet werden. Das Verarbeitungsverzeichnis ist daher zumindest jedem Unternehmen, das Arbeitnehmer beschäftigt, dringend anzuraten.

Das Verarbeitungsverzeichnis muss neben den personenbezogenen Daten selbst auch den Zweck der Verarbeitung der Daten und die Namen derjenigen Personen enthalten, denen die Daten offengelegt werden. Darüber hinaus sind Datenübermittlungen ins Ausland zu dokumentieren und – wenn möglich – Fristen für eine Löschung in das Verzeichnis aufzunehmen. Auch organisatorische Maßnahmen, die den Schutz der Daten sicherstellen sollen, müssen in dem Verzeichnis dokumentiert werden. Das Verzeichnis ist auf Verlangen der Datenschutzbehörde vorzuweisen.

Datenübermittlung in Drittstaaten

In internationalen Konzernen stellt sich regelmäßig die Frage, ob personenbezogene Daten in Drittstaaten übermittelt werden dürfen. Hierbei handelt es sich um Staaten, die weder der EU angehören noch zu den Staaten des Europäischen Wirtschaftsraums (EWR) zählen. Wichtige Drittstaaten sind etwa die USA, China oder Russland. Nach der DSGVO ist allein die Europäische Kommission befugt, in Form sogenannter Angemessenheitsbeschlüsse die Datensicherheit in dem in Frage kommenden Drittstaat zu bewerten und die Zulässigkeit der Datenübermittlung verbindlich festzulegen. Zur DSGVO selbst gibt es noch keine entsprechenden Beschlüsse. Bis solche erlassen werden, gelten die bestehenden Beschlüsse zur Datenschutzrichtlinie. Demnach ist beispielsweise die Übermittlung personenbezogener Daten in die USA aufgrund des zwischen der EU und den USA vereinbarten Abkommens „EU-US Privacy Shield" nur dann zulässig, wenn das empfangende Unternehmen in einer vom amerikanischen Handelsministerium veröffentlichten Liste, ähnlich der früheren „Safe Harbour"-Liste, enthalten ist. Für die Schweiz liegt derzeit zum Beispiel ein Angemessenheitsbeschluss vor, nicht aber für Länder wie beispielsweise China und Russland.

Wann ist ein Datenschutzbeauftragter zu bestellen?

Bislang waren Organisationen nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Mit der DSGVO ändert sich dies. Fortan muss ein Datenschutzbeauftragter bestellt werden

- für öffentliche Stellen und Ämter
- wenn die Kerntätigkeit des Unternehmens in der umfangreichen und regelmäßigen Überwachung (zum Beispiel ASFINAG) oder
- in der Verarbeitung sensibler Daten (zum Beispiel Krankenanstalt) liegt.

Aufgrund der umfangreichen Verpflichtungen, die die DSGVO vorsieht, sind Unternehmen gut beraten, die Stelle eines Datenschutzbeauftragten zu besetzen, auch wenn deren Einrichtung im Einzelfall nicht verpflichtend ist. Geldbußen, die die Datenschutzbehörde im Fall von Verstößen gegen die DSGVO verhängt, sind Verwaltungsstrafen. Als solche richten sie sich an die Geschäftsführung, wobei alle Mitglieder zur ungeteilten Hand haften. Für die Einhaltung der datenschutzrechtlichen Bestimmungen kann theoretisch ein „verantwortlich Beauftragter" im Sinne von § 9 des Verwaltungsstrafgesetzes (VStG) bestellt werden, der im Fall eines Verstoßes von der Behörde anstelle des Arbeitgebers beziehungsweise der Geschäftsführer bestraft wird.

Ob eine solche Bestellung wirklich wirksam erfolgen kann, ist offen. Es scheint insbesondere fraglich, ob die für verantwortlich Beauftragte notwendige „Anordnungsbefugnis" für

ein ganzes Unternehmen (Geschäftsführer) oder auch nur eine Abteilung realistischerweise vorliegen kann. Denn dem Anspruch, die Daten eines gesamten Unternehmens – oder auch nur einer Abteilung – im Griff zu haben, wird wohl kaum jemand gerecht werden können. Angesichts der monströsen Strafdrohungen bei Verstößen gegen die Verpflichtungen aus der DSGVO beziehungsweise dem DSG neu, die bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen können, werden Datenschutzbeauftragte ohnehin nicht gerne einer Bestellung als verantwortlich Beauftragter zustimmen.

Meldung von Datenschutzverletzungen

Arbeitgeber (in der Terminologie der DSGVO „Verantwortliche") müssen der Datenschutzbehörde unverzüglich, möglichst binnen 72 Stunden melden, wenn der Schutz von personenbezogenen Daten verletzt wurde (zum Beispiel durch einen Hackerangriff oder ein Datenleck) und dies zu einem Risiko für die Rechte und Freiheiten davon betroffener Personen führt (zum Beispiel Rufschädigung, Gefahr finanzieller Verluste oder Verlust der Vertraulichkeit von Daten, die einem Berufsgeheimnis unterliegen). In solchen Fällen muss der Verantwortliche (der Arbeitgeber) auch die betroffene Person von der Datenschutzverletzung in Kenntnis setzen. Nicht nur der „Data Breach" (bei ungenügenden technischen Vorkehrungen), sondern auch die Verletzung der Meldepflichten führt zu einer gesonderten Verwaltungsstrafe.

Welche Rechte haben Arbeitnehmer?

Sind Arbeitnehmer von der Verarbeitung ihrer Daten betroffen, können sie schon jetzt vom Arbeitgeber jederzeit Auskunft, Berichtigung und Löschung ihrer Daten verlangen. Darüber hinaus können sie auch einer bereits erfolgten Datenverarbeitung widersprechen. Mit dem Inkrafttreten der der DSGVO kommen weitere Rechte hinzu:

a. Das Recht auf Einschränkung der Verarbeitung: Bestreitet ein Arbeitnehmer die Richtigkeit bestimmter Daten oder wurden seine Daten unrechtmäßig verarbeitet, indem beispielsweise die Verarbeitung die Grenzen einer Zustimmungserklärung überschritten hat, kann er für die Dauer der Klärung eine Einschränkung der Verarbeitung verlangen. Die Daten werden dann nicht gelöscht, sondern nicht weiter verarbeitet. Dies kann etwa durch eine Einschränkung des (technischen) Zugangs zu den Daten bewirkt werden.

b. Das Recht auf Datenübertragbarkeit ist kein eigentliches Schutzrecht, sondern erleichtert es Betroffenen, Daten von einem Verarbeiter (Arbeitgeber) zum nächsten zu transferieren. Dieses Recht ist grundsätzlich eher auf Konsumenten und weniger auf Arbeitnehmer zugeschnitten. Es kann jedoch beispielsweise bei Arbeitgeberwechseln herangezogen werden, wenn der wechselnde Arbeitnehmer sich selbstständig macht und zum Beispiel Kundendaten (freilich mit deren Zustimmung) in sein neues Büro transferieren möchte.

Darüber hinaus können sich Arbeitnehmer bei Verstößen gegen die DSGVO der Datenschutzbehörde beschweren und auf dem (Zivil-)Rechtsweg beispielsweise Schadenersatz geltend machen.

Die Rechte des Betriebsrats

Artikel 88 DSGVO erlaubt es den Mitgliedstaaten, im arbeitsrechtlichen Kontext durch nationale Regelungen spezifischere Schutzvorschriften in Form von Gesetzen oder Kollektivvereinbarungen zu erlassen. Der österreichische Gesetzgeber macht mit § 11 Datenschutzgesetz neu davon Gebrauch und erklärt das gesamte Arbeitsverfassungsgesetz (ArbVG) zu einer solchen spezifischeren Schutzvorschrift im Sinne des ArbVG. Ausgenommen ist § 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG), in dem bislang die einzelvertragliche Zustimmung zu bestimmten Formen der Datenverwendung geregelt ist. Damit erhält der Datenschutz in Österreich neben der vertraglichen eine kollektivrechtliche Ebene und mit dem Betriebsrat sozusagen eine weitere Kontrollinstanz. Wie mit dem Spannungsfeld zwischen Arbeitnehmerinteressen und Betriebsratsinteressen umzugehen sein wird, ist offen. Im Sinne der DSGVO dürfen die Betroffenenrechte durch Befugnisse des Betriebsrats nicht eingeschränkt werden. Verlangt also beispielsweise der Arbeitnehmer eine Einschränkung der Verarbeitung gemäß Artikel 18 DSGVO, darf ab diesem Zeitpunkt wohl auch der Betriebsrat keine Einsicht mehr in die betroffenen Daten nehmen, auch wenn das ArbVG ihm diese nach bisheriger Rechtslage erlauben würde.

Ausblick für die Praxis

Österreichische Arbeitgeber sollten aufgrund der tiefgreifenden Veränderungen und der empfindlichen Sanktionen spätestens jetzt mit der Vorbereitung auf das Inkrafttreten der Datenschutz-Grundverordnung beginnen. Wie wichtig die Erstellung eines Verzeichnisses für Verarbeitungstätigkeiten, die Datenpflege, die Gestaltung und das Einholen von Zustimmungserklärungen sowie die Bestellung eines Datenschutzbeauftragten sind, hat der Überblick gezeigt. Darüber hinaus sollten sich Unternehmen insbesondere zu folgenden Fragen Gedanken machen:

- Wie ist mit Bewerberdaten umzugehen? Wann müssen sie gelöscht werden?
- Was passiert, wenn ein Arbeitsnehmer der Verarbeitung seiner Daten widerspricht?
- Wie wird sichergestellt beziehungsweise ist überhaupt sicherzustellen, dass keine Daten aus privaten E-Mails und Logfiles von Arbeitnehmern verarbeitet werden? Liegt eine wirksame Zustimmungserklärung des Arbeitnehmers (allenfalls auch eine Betriebsvereinbarung) vor?
- Wie ist mit Daten ausgeschiedener Mitarbeiter umzugehen?
- Welche Datenschutzvereinbarungen muss es mit Vertragspartnern geben, denen personenbezogene Daten übermittelt werden?
- Werden von Arbeitnehmern Bild- und Videodaten verarbeitet? Zu welchen Zwecken? Gibt es dafür eine Zustimmungserklärung?
- Werden Daten von Arbeitnehmern in Social-Media-Plattformen oder in E-Mail-Aussendungen sowie auf Weihnachtskarten veröffentlicht? Liegt eine Zustimmungserklärung dafür vor?

Der Katalog kann sehr weit fortgesetzt werden. Ein Datenschutzaudit und die Implementierung der notwendigen Änderungen sind ab sofort dringend empfohlen.