Greiter
Pegger
Kofler

Rechtsanwälte

Mitarbeiter-Datenschutz neu

kompakt und praxisnah

RA Dr. Herwig Frei

Stand: Oktober 2018

Impressum
Medieninhaber und Herausgeber:
Greiter Pegger Kofler & Partner Rechtsanwälte

Maria-Theresien-Straße 24
6020 Innsbruck, Austria

Telefon: +43 512 57 18 11
Fax: +43 512 58 49 25

office@lawfirm.at
www.lawfirm.at

Mitarbeiter-Datenschutz neu

kompakt und praxisnah

RA Dr. Herwig Frei

Über den Autor
Rechtsanwalt Dr. Herwig Frei ist Partner der Kanzlei Greiter Pegger Kofler & Partner. Er berät und vertritt im privaten und öffentlichen Wirtschaftsrecht. Zu seinen Tätigkeitsschwerpunkten gehören Fragen im und rund um das Arbeitsrecht.

Greiter Pegger Kofler | Rechtsanwälte

1. Grundsätzliches zum Mitarbeiter-Datenschutz

1.1. Ausgangslage

Beschäftigt ein Unternehmen Mitarbeiter, hat man es unweigerlich mit Personaldaten (Human Ressource- bzw. HR-Daten) zu tun, die auf vielfältige Weise zu verschiedensten Zwecken (unjuristisch gesprochen) „behandelt" werden.

Für den Umgang mit solchen Personaldaten gibt es ein doppeltes rechtliches Regelwerk, nämlich im „klassischen" Arbeitsrecht sowie im Datenschutzrecht. Hier geht es in erster Linie um die datenschutzrechtliche Komponente, also den Mitarbeiter-Datenschutz. Selbstverständlich werden aber auch die Schnittstellen bei Personaldaten und ihrer Verarbeitung zum herkömmlichen Arbeitsrecht (Betriebsverfassung, Arbeitsvertragsrecht) etwas näher beleuchtet.

1.2. Neues Datenschutzrecht seit 25.05.2018 (DSGVO, DSG neu)

Seit 25.05.2018 gilt in der gesamten EU und damit auch in Österreich die Datenschutz-Grundverordnung (VO 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz „DSGVO"). Flankiert wird die DSGVO durch das österreichische Datenschutzgesetz – DSG. So wurde (vor allem) mit dem Datenschutz-Anpassungsgesetz 2018 (BGBl I 2017/120) und dem Datenschutz-Deregulierungs-Gesetz 2018 (BGBl I 2018/24) das alte bisherige Datenschutzgesetz aus 2000 mit Wirksamkeit 25.05.2018 an die DSGVO angepasst (kurz „DSG neu").

Die DSGVO enthält keine speziellen Regelungen zum Arbeitnehmer-Datenschutz. Im Art. 88 DSGVO ist lediglich vorgesehen, dass die EU-Mitgliedstaaten für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext spezifischere Regelungen erlassen können. Von dieser sog. Öffnungsklausel hat der österreichische Gesetzgeber aber letztlich (nach einem legistischen Zick-Zack-Kurs) nicht, auch nicht bloß teilweise Gebrauch gemacht.

Es gibt kein spezielles, gleichsam maßgeschneidertes Arbeitnehmer-Datenschutzrecht, und zwar weder auf EU-Ebene noch in Österreich. Für den Datenschutz von HR-Daten gelten also (grundsätzlich) „nur" die (ganz) allgemeinen Regelungen im neuen Datenschutzrecht (DSGVO, DSG neu).

Über das allgemeine Datenschutzrecht neu gibt das Kanzleiheft „Datenschutzrecht – Überblick und Umsetzung (mit Checkliste)" unseres Kanzleipartners RA Dr. Georg Huber, LL.M. einen umfassenden Überblick. Es wird angeraten, diese Broschüre vor bzw. begleitend mit jener, die Sie jetzt in Händen halten, zu lesen. Die Ausführungen in der hiesigen Broschüre verstehen sich „ohne Gewähr", sie dienen nur zu Ihrer ersten rechtlichen Groborientierung im Mitarbeiter-Datenschutz und können eine fundierte Rechtsberatung im Einzelfall klarerweise nicht ersetzen. Überhaupt: Im neuen Datenschutzrecht ist noch einiges/vieles (zu?) offen und unklar, für gesicherte Aussagen auf Basis gefestigter Rechtsprechung ist das neue europäische und österreichische Datenschutzregime einfach noch zu jung!

1.3. Die datenschutzrechtlichen Akteure im Arbeitsverhältnis

Das Datenschutzrecht geht von einem simplen Rollenmuster aus. Der datenschutzrechtliche „Verantwortliche" (alte Terminologie „Auftraggeber") steht dem „Betroffenen" gegenüber. Betroffener ist derjenige (natürliche Person), dessen Daten verarbeitet werden. Der Verantwortliche verarbeitet die Daten des Betroffenen.

Ausgehend von dieser typischen Rollenverteilung haben wir es im Arbeitsverhältnis mit folgenden datenschutzrechtlichen Akteuren/Protagonisten zu tun:

Arbeitgeber (AG): Er ist der Verantwortliche. Als Träger des Unternehmens mitsamt der Belegschaft verarbeitet er im Rahmen seines Geschäftsbetriebes nicht nur Daten seiner Kunden und Lieferanten, sondern auch seiner Mitarbeiter. Die Unternehmensgröße (Mitarbeiterzahl) spielt keine Rolle, das neue Datenschutzrecht gilt daher nicht nur für Großkonzerne, sondern gleichermaßen (1:1) auch für klein(er)e Unternehmen (KMUs, Start-Ups) und unabhängig von der Rechtsform der Unternehmen (AG, GmbH, Personengesellschaft, Einzelunternehmer etc.).

Arbeitnehmer (AN): Jeder einzelne AN ist mit seinen Daten Betroffener. Gemeint sind die AN (Arbeiter, Angestellte, Lehrlinge), die in einem echten, abhängigen (persönliche Abhängigkeit) Dienstverhältnis stehen, und zwar gleichgültig ob in Voll- oder Teilzeit, ob über oder unter der Geringfügigkeitsgrenze.

Differenziert ist der datenschutzrechtliche Status von (echten) freien Dienstnehmern („freelancer") und (echten) Werkvertragsunternehmern (auf Werkvertragsbasis tätige Auftragnehmer) zu sehen. Diese können, wenn sich zB das Unternehmen (Unternehmensträger) ihrer bei seiner Leistungserbringung gegenüber den Kunden bedient, insoweit auch Auftragsverarbeiter sein.

Betriebsrat: Gibt es im Unternehmen einen Betriebsrat, so ist dieser in der Regel datenschutzrechtlich als „Dritter" einzustufen (wenn ihm zB Mitarbeiterdaten zwecks Ausübung seiner Informations- und Kontrollrechte gegeben werden). Verarbeitet der Betriebsrat jedoch selbst, dh autonom Daten der von ihm vertretenen AN, so wird er insoweit zum Verantwortlichen.

Externe/ausgelagerte Dienste: Werden beispielsweise HR-Daten in der IT-Wolke (cloud computing) verarbeitet, handelt es sich bei diesem externen Dienstleister (IT-Cloud-Anbieter) datenschutzrechtlich um einen Auftragsverarbeiter (alte Terminologie „Dienstleister"). Auftragsverarbeiter ist eine natürliche oder juristische Person oder Behörde, die im Auftrag und über Weisung des Verantwortlichen (hier: des AG) personenbezogene Daten verarbeitet.

Spezialfall externer Lohn- und Gehaltsverrechner: Die Abgrenzung zwischen einem eigenständigen Verantwortlichen und einem Auftragsverarbeiter ist immer wieder schwierig (Graubereich). In einem Fall aus Jänner 2018 (Lohnabrechnung für parlamentarische Mitarbeiter im Auftrag der Parlamentsdirektion durch eine *externe Steuerberatungskanzlei*) hat die Datenschutzbehörde entschieden (Entscheidung vom 22.01.2018, DSB-D122.767/0001-DSB/2018), dass es sich bei einem *Steuerberater/Wirtschaftstreuhänder* aufgrund seiner beruflichen Selbständigkeit und Eigenverantwortlichkeit datenschutzrechtlich um einen (vormals) Auftraggeber, sprich nunmehr um einen Verantwortlichen handelt.

Gewerkschaft, Arbeiterkammer, Arbeitsgericht, Arbeitsinspektorat, AMS, Sozialversicherungsträger, betriebliche Vorsorgekasse, Pensionskasse etc.: Kommt es zB zu einer arbeitsrechtlichen Auseinandersetzung (vorgerichtliche Interventionsphase, Arbeitsgerichtsprozess) und fließen Mitarbeiterdaten an diese Institutionen, so handelt es sich bei diesen in der Regel um Dritte/Empfänger. Gleiches gilt bei einem Arbeitsunfall, der dem Arbeitsinspektorat gemeldet wird (Meldepflicht), oder bei einer Bescheinigung an das AMS aus Anlass der Beendigung eines Arbeitsverhältnisses.

1.4. Personaldaten und ihre Gruppierung

Das Datenschutzrecht schützt (natürliche) Personen mit ihren personenbezogenen Daten. Der Begriff ist sehr weit gefasst. Darunter fallen alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Als identifizierbar wird eine natürlich Person angesehen, die (Zitat VO-Wortlaut Art. 4 Z 1) *„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."*

Erfasst sind nicht nur Daten im engeren Sinne, sondern auch Textdokumente (personenbezogene Korrespondenz, Aktenvermerke), Bilddaten (Fotos, Videos bei zB Videoüberwachung) und Tondaten (Audiodateien).

Nicht erfasst sind sohin lediglich anonyme Daten, die nicht, also auch nicht „über Umwege", Rückschlüsse auf eine Person zulassen bzw. rückführbar sind.

Innerhalb der personenbezogenen Daten gibt es zwei Gruppen, nämlich die *„normalen" (nichtsensiblen)* Daten sowie die *besonderen Kategorien personenbezogener Daten* (Art. 9 Abs. 1 DSGVO). Letztere sind besonders heikel, sie lassen sich von der Systematik her unterteilen in *sensible* und *strafrechtlich relevante* Daten (Art. 10 DSGVO).

Zu den sensiblen Daten gehören Daten zur rassischen und ethnischen Herkunft, zu politischen,

religiösen und weltanschaulichen Überzeugungen, zur Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten sowie Daten zum Sexualleben.

Umgelegt auf das Arbeitsverhältnis (praktische Beispiele) bedeutet dies etwa konkret:

„Normale" Mitarbeiterdaten: zB Name, Titel, Adresse, Geschlecht, Geburtsdatum/Alter, Familienstand, Telefonnummer, E-Mail-Adresse, berufliche Kontaktdaten des AN, Bankverbindung, Führerscheindaten, Einkommen, Vermögen, Sozialversicherungsnummer (könnte fraglich sein), E-Mail- und Internet-Nutzungsdaten beim AN-Computer ([dynamische] IP-Adresse, generierte Log-Files etc.), idR Bewegungsdaten/Standortdaten (GPS-Ortung oder trackingfähige/personenregistrierte Smartphones/Diensthandys, die eine Ortung des Mitarbeiters ermöglichen), Mitarbeiterfotos auf der Firmen-Homepage oder von Firmenausflügen in einer Mitarbeiter- oder Kundenzeitschrift, Interessen, Vorlieben und Fähigkeiten des AN (relevant zB bei sog. Skillsdatenbanken/Talentmanagementsystemen) usw.

Sensible Mitarbeiterdaten: zB Gewerkschaftszugehörigkeit (Abzug und Abfuhr des ÖGB-Mitgliedsbeitrages durch AG bei Lohn- und Gehaltsabrechnung), Religionsbekenntnis (relevant für zusätzlich arbeitsfreien Tag, Stichwort „Karfreitag"), Nationalität (könnte fraglich sein), Gesundheitsdaten (Krankenstandsaufzeichnungen; Behinderungen; in ärztlichen Gutachten enthaltene Daten zur Gesundheitssituation eines AN), Gesichtsbilder (zB bei Zutrittskontrollsystemen wie Iris-Scan), daktyloskopische Daten/Fingerabdruck (zB bei einem biometrischen Zeiterfassungssystem mittels Fingerscanner) usw.

Es kommt immer wieder vor, dass sich sensible Daten gleichsam „versteckt" im Personalakt befinden.

Nach österreichischem Gentechnikgesetz (§ 67 Abs. 1 GTG) sind Gentests an AN und Bewerbern (Arbeitssuchende) ausdrücklich verboten (zulässige nationale Beschränkung). Von diesem Verbot sind auch das Verlangen nach Abgabe und die Annahme von Körpersubstanz für genanalytische Zwecke umfasst.

Strafrechtlich relevante Mitarbeiterdaten: vor allem Strafregisterbescheinigung betreffend Vorstrafen von AN oder Bewerbern („Leumundszeugnis")

1.5. Dateisystem und Personalakt

Die DSGVO erfasst sowohl die manuelle (händische) als auch die automatisierte Verarbeitung personenbezogener Daten, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Dateisystem ist (Zitat VO-Wortlaut Art. 4 Z 6) *„jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird"*.

Nach dem Erwägungsgrund 15 fallen Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, nicht in den Anwendungsbereich der DSGVO.

Umgelegt auf den Personalakt heißt dies: Der digitale/elektronische Personalakt („E-Personalakt") ist immer auch ein Dateisystem und daher DSGVO-geschützt.

Beim (lediglich) manuell/händisch geführten Personalakt lässt sich diese Frage nicht generell beantworten. Meines Erachtens ist zu unterscheiden, ob der Papier-Personalakt irgendwie strukturiert ist oder nicht (zB durch alphabetische, thematische, chronologische Sortierung oder Sortierung nach einem bestimmten Suchkriterium). Ein unstrukturierter bzw. nicht in besonderer Weise strukturierter Papier-Personalakt (vgl. VfGH 10.12.2014, B 1187/2013) dürfte nicht als Dateisystem zu werten und daher nicht DSGVO-geschützt sein.

Dennoch heißt das nicht, dass der „papierene AN" hier schutzlos ist bzw. der AG hier „Narrenfreiheit" hat. Der „papierene AN" kann, insbesondere gestützt auf das mit Drittwirkung ausgestattete und damit auch gegenüber einem privaten AG beanspruchbare Grundrecht auf Datenschutz (§ 1 Abs. 1 DSG neu), bestimmte Ansprüche (zB auf physische Vernichtung/Schwärzung etc. unrechtmäßiger Teile des Personalaktes) gegen den AG geltend machen.

1.6. Wann werden Personaldaten bereits verarbeitet?

Der Verarbeitungsbegriff ist ein immens weiter. Darunter fällt jeder manuelle oder automatisierte

Vorgang im Zusammenhang mit personenbezogenen Daten wie zB das Erheben, Erfassen, Ordnen, Aufbewahren/Speichern, Anpassen, Verändern, Auslesen, Abfragen, Übermitteln, Verbreiten, Abgleichen, Verknüpfen, Löschen etc. Alles, was in der tagtäglichen Personaladministration typischerweise passiert, ist also ein datenschutzrechtlich relevanter Verarbeitungsvorgang.

2. Erlaubnisgründe für die Verarbeitung von Mitarbeiter- und Bewerberdaten mit praktischen Fallbeispielen

2.1. Tipp vorab: Mit AN-Einwilligungen sparsamst umgehen!

Um gleich vorweg mit einem immer wieder gehörten Irrglauben (Mythos) aufzuräumen: Nicht jede Datenverarbeitung im Unternehmen erfordert eine (vorherige) Einwilligung des Betroffenen, also bei Mitarbeiterdaten des jeweiligen AN!

Die Einwilligung ist nur eine von mehreren möglichen Rechtsgrundlagen (Erlaubnis- bzw. Rechtfertigungsgründen). Da eine Einwilligung, um gültig zu sein, nicht nur informiert, sondern auch freiwillig erfolgen muss und an diese Freiwilligkeit angesichts des (grundsätzlich unterstellten) Abhängigkeitsverhältnisses in AG-AN-Beziehungen hohe Anforderungen gestellt werden, ist zu empfehlen, sich beim Beschäftigtendatenschutz nach Möglichkeit auf andere Rechtsgrundlagen zu stützen. Dazu kommt die praktisch-simple Überlegung, dass erteilte Einwilligungen jederzeit grundlos für die Zukunft widerrufen werden können, sodass im Falle eines Widerrufs durch den AN die Datenverarbeitung gestoppt und die betreffenden Mitarbeiterdaten gelöscht werden müssen. Dieser latente Unsicherheitsfaktor ist keine gute Basis für laufende Personalarbeit. Dann, also in Not einen anderen Rechtfertigungsgrund „aus dem Hut zaubern“ und sich darauf berufen zu wollen, könnte rechtlich problematisch sein (wegen Intransparenz).

2.2. Rechtliche Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO, für sensible Daten Art. 9 Abs. 2 lit. b DSGVO)

Datenverarbeitungen, die zur Erfüllung einer rechtlichen (gesetzlichen, nicht bloß vertraglichen) Verpflichtung nötig sind, sind allein schon deswegen („automatisch“) legitimiert. Gerade in der Abwicklung/Administration eines Arbeitsverhältnisses existieren zahlreiche arbeits-, sozialversicherungs-, abgaben- bzw. (lohn)steuerrechtliche Verpflichtungen, denen ein Arbeitgeber unterliegt. Dies sind beispielsweise und stichwortartig (kein Anspruch auf Vollständigkeit) nachstehende Melde-, Aufzeichnungs- bzw. Dokumentationspflichten und Auskunftspflichten gegenüber Sozialversicherungsträgern, Finanzbehörden und sonstigen Behörden/Institutionen:

- An- und Abmeldung des AN zur Sozialversicherung/GKK (§§ 33 ff ASVG)
- Ausstellung eines Dienstzettels/Arbeitsvertrages mit gesetzlich vorgeschriebenen Mindestinhalten (§ 2 AVRAG)
- Arbeitszeitaufzeichnungen (§ 26 AZG)
- Urlaubsaufzeichnungen (§ 8 UrlG)
- Daten/Aufzeichnungen iZm Krankenständen (§ 8 AngG, EFZG, ASVG)
- Aufzeichnungen/Berichte über Arbeitsunfälle (ASchG)
- Lohn-, Gehalts- und Entgeltabrechnung (zB Rechtsgrundlage Lohnzettel § 78 Abs. 5 EStG 1988; Fahrtenbücher; AG als Drittschuldner gegenüber betreibendem Gläubiger und Exekutionsgericht bei Gehaltsexekution)
- Abfertigung „alt“ (AngG, ArbAbfG) und „neu“ (betriebliche Vorsorgekasse/BMSVG)
- Betriebspensionen/Pensionskasse (BPG/PKG)
- Bestellung eines AN zum gewerberechtlichen Geschäftsführer des Unternehmens: Meldung seiner Daten an die Gewerbebehörde gemäß § 39 Abs. 4 GewO
- diverse Informations- und Auskunftspflichten gegenüber dem Betriebsrat (ArbVG)
- Auskunfts- und Meldepflichten bei begünstigten Behinderten (§ 16 BEinstG)
- Duldung von und Mitwirkung an (amtswegigen) GPLA-Prüfungen durch den AG

Eine rechtliche Verpflichtung zu bestimmten Personaldaten-Verarbeitungen kann sich für den AG auch aus „Kollektivvereinbarungen“ (Kollektivvertrag, Betriebsvereinbarung) ergeben.

Dieser Rechtfertigungsgrund taugt sowohl für „normale“ wie für sensible Mitarbeiterdaten.

Bei ihm ist natürlich auch der (strikte) Zweckbindungsgrundsatz laut DSGVO zu beachten, wonach Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet/erhoben werden dürfen. Am Beispiel von Krankenständen heißt dies etwa: Firmeninterne Krankenstandsstatistiken über Häufigkeit, Dauer und Lage von Krankenständen der Mitarbeiter (zB zum Zwecke der Mitarbeiterbeurteilung) sind nicht vom bezüglichen gesetzlichen Zweck iZm Krankenständen (Meldung an SV-Träger, Lohnverrechnung) erfasst.

2.3. Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO)

Dieser Erlaubnisgrund liegt dann vor, wenn Daten zur Erfüllung, d.h. zum/zur Abschluss, Durchführung, Änderung und Beendigung eines mit dem Betroffenen geschlossenen Vertrages verarbeitet werden müssen. Im Arbeitsleben ist dieser Vertrag der Arbeitsvertrag (oder sonstige arbeitsrechtliche Vereinbarungen) zwischen AG und AN.

Beispiel: Damit der AG das Gehalt (bargeldlos) zahlen, sprich den Arbeitsvertrag in punkto Entgeltpflicht erfüllen kann, benötigt er die Bankdaten des AN.

Mit „Erfüllung Arbeitsvertrag“ lässt sich nicht alles und jedes im vertraglichen Umfeld rechtfertigen. So ist im Beschäftigtenkontext zu unterscheiden, in welchem Umfang eine Datenverarbeitung für die Erfüllung des Vertrages (wirklich) notwendig (Notwendigkeitserfordernis; Zweckmäßigkeit genügt nicht) ist und welche Nebenabreden nicht den eigentlichen Vertragszweck betreffen. So sind zB Regelungen über den privaten E-Mail-Verkehr des Mitarbeiters oder die Videoüberwachung seines Arbeitsplatzes für die Durchführung des Arbeitsverhältnisses nicht notwendig und daher in Datenschutzhinsicht nur rechtens, wenn sie auf eine andere Rechtsgrundlage gestützt werden können.

Mit Stellenbewerbern gibt es klarerweise (noch) keinen Vertrag, man ist also im Stadium vor einem Arbeitsvertrag. Die Rechtsgrundlage Vertragserfüllung deckt (aber) auch eine Datenverarbeitung ab, die erforderlich ist für vorvertragliche Maßnahmen, wenn diese auf Initiative der betroffenen Person erfolgen. Dies ist bei Bewerbungen (Initiativbewerbungen, auf ausgeschriebene Stelle) der Fall. Nach Ablehnung sind die Daten des (erfolglosen) Bewerbers mit einem gewissen Nachlauf (Stichwort: Klagsfristen bis zu 6 Monaten nach GlBG) zu löschen/anonymisieren, es sei denn, der Bewerber hat ausdrücklich in ein Evidenthalten seiner Daten für einen späteren Auswahlprozess (Evidenzliste) eingewilligt.

Die Verarbeitung sensibler Daten kann nie mit „Vertragserfüllung/vorvertragliche Maßnahmen“ gerechtfertigt werden.

2.4. Überwiegende berechtigte Interessen des AG (Art. 6 Abs. 1 lit. f DSGVO)

Dies ist wohl der am schwierigsten zu greifende Erlaubnisgrund. Gemeint sind jene Fälle, in denen die Datenverarbeitung zur Wahrung berechtigter Interessen des Datenverarbeiters (hier: des AG) erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person (hier: des AN), die den Schutz personenbezogener Daten erfordern, überwiegen.

Es ist also zwingend im jeweiligen Einzelfall eine Interessenabwägung (gegenläufige Interessen) vorzunehmen. Einen Anhaltspunkt für den Bewertungsmaßstab liefert der Erwägungsgrund 48 der DSGVO. Dort heißt es wortwörtlich: *„Verantwortliche, die Teil einer Unternehmensgruppe … sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.“*

Diese Erwägungen (beachtliche Auslegungshilfe) sind also für Konzerne interessant und bedeutsam. Dennoch muss man eines festhalten: Die DSGVO kennt kein Konzernprivileg, also keinen allgemeinen Erlaubnistatbestand für eine konzernweite Datenweitergabe: Jede Daten-Übermittlung innerhalb eines Konzerns bedarf einer Rechtfertigung nach den allgemeinen „Spielregeln“ (Erlaubnistatbestände).

Auf den Rechtfertigungsgrund „überwiegende berechtigte Interessen“ (vor allem Interesse an

einem reibungslosen Geschäftsablauf) könnte ein AG zB in folgenden Fällen greifen bzw. zu greifen versuchen:

- Mitarbeiterausweise inklusive Mitarbeiterfoto
- Veröffentlichung beruflicher Kontaktdaten im Firmen-Intranet
- Veröffentlichung beruflicher Kontaktdaten (ohne Mitarbeiterfoto) auf der Firmen-Website, vor allem bei Mitarbeitern mit Außenkontakt (Möglichkeit der [erleichterten] Kontaktaufnahme durch Kunden und Lieferanten)
- Datenverarbeitung zum Zwecke der Verwaltung und Sicherheit des Firmen-IT-Systems (Verwaltung von Benutzerkennzeichen, Zuteilung von Hard- und Software an Systembenutzer etc.)
- Maßnahmen zum Schutz der Mitarbeiter (zB mittels Videoüberwachung, Telefonaufzeichnungen bei Beschwerdefällen etc. [neben dem Kundenschutz])
- Übermittlung der wichtigsten Personaldaten (inklusive Gehaltsdaten) des Managements an beherrschende Unternehmen

2.5. Einwilligung des AN (Art. 6 Abs. 1 lit. a DSGVO, für sensible Daten Art. 9 Abs. 2 lit. a DSGVO)

Wie schon in 2.1. thematisiert, sollte der AG eine Einwilligung des AN nur dann einholen, wenn keiner der vorgenannten Rechtfertigungsgründe greift oder diese zu riskant erscheinen (bei Grenzfällen).

Damit eine Einwilligung des AN gültig ist, ist Folgendes zu beachten:

- Der AN muss wissen, wozu er einwilligt (konkretes Wofür und Wofür-Nicht, welche seiner Daten, allfällige Datenempfänger, maximale Speicherdauer). Pauschaleinwilligungen ohne Angabe des genauen Verarbeitungszweckes sind unwirksam. Bloß allgemeine Zweckumschreibungen wie zB Personalverwaltung, HR-Management etc. genügen nicht.
- Für jede einzelne Datenverarbeitung ist eine separate Einwilligung nötig (keine „Sammeleinwilligung“ oder gar Einwilligung „auf Vorrat“).
- Die Einwilligung muss leicht verständlich formuliert sein und über die Möglichkeit des jederzeitigen Widerrufs informieren.
- Schon aus Beweisgründen empfiehlt sich (nur) eine schriftliche Einwilligung.
- Die Einwilligung des AN zu Datenverarbeitungen, die für das Arbeitsverhältnis lediglich nützlich sind, darf nicht mit dem Abschluss oder der weiteren Aufrechterhaltung des (Arbeits)Vertrages verknüpft werden („Koppelungsverbot“, echte Freiwilligkeit im Sinne von voller Wahlfreiheit).

  So wäre es etwa möglich, dass der AN in einer separaten, zum Arbeitsvertrag hinzutretenden Vereinbarung in verhältnismäßige Kontrollen seiner Internet- und E-Mail-Nutzung einwilligt, wenn eine Privatnutzung in bestimmtem (angemessenem) Umfang erlaubt ist.

Bestehende Einwilligungserklärungen nach altem Datenschutzrecht (alte Diktion „Zustimmung“ statt „Einwilligung“) sind und bleiben, sofern sie der neuen Rechtslage entsprechen, weiter gültig. Solche alten Einwilligungserklärungen sollten also kritisch durchforstet werden. Besteht ein Anpassungsbedarf (weil zB seinerzeit bei Abgabe der Einwilligungserklärung nicht über das jederzeitige Widerrufsrecht informiert wurde), sollte unbedingt eine neue Zustimmungserklärung des betroffenen AN eingeholt werden.

Dieser Rechtfertigungsgrund taugt sowohl für nicht-sensible als auch für sensible Daten. Bei sensiblen Daten hat die Einwilligung ausdrücklich zu erfolgen.

3. Betriebsrat, Betriebsvereinbarung und Datenschutz

3.1. Befugnisse des Betriebsrates aufgrund der Betriebsverfassung

In Betrieben mit Betriebsrat (BR) kommen der Belegschaftsvertretung nach der Betriebsverfassung (II. Teil im ArbVG) diverse Rechte/Befugnisse (Überwachung, Intervention, Information,

Beratung, Zustimmung) zu.

§ 91 Abs. 2 ArbVG regelt die Informationspflicht des Betriebsinhabers (AG) über personenbezogene Mitarbeiterdaten wie folgt:

„Der Betriebsinhaber hat dem Betriebsrat Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht. Dem Betriebsrat ist auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen. Sofern sich nicht aus § 89 oder anderen Rechtsvorschriften ein unbeschränktes Einsichtsrecht des Betriebsrates ergibt, ist zur Einsicht in die Daten einzelner Arbeitnehmer deren Zustimmung erforderlich.“

Vom verwiesenen § 89 ArbVG sind vor allem die BR-Befugnisse laut Z 1 von Relevanz, nämlich das Recht auf Einsichtnahme in die Lohn- und Gehaltslisten der vom BR vertretenen Mitarbeiter und in vom AG verpflichtend zu führende Arbeitnehmer-Aufzeichnungen (primär Arbeitszeit, Urlaub).

Zu den Zustimmungsrechten des Betriebsrates gehören auch Zustimmungsrechte in Form des Abschlusses von Betriebsvereinbarungen. Zentral sind hier vor allem 3 Anwendungsfälle, nämlich (erstens) Betriebsvereinbarungen über Kontrollmaßnahmen bzw. technische Systeme zur Kontrolle von Arbeitnehmern, welche deren Menschenwürde berühren (§ 96 Abs. 1 Z 3 ArbVG; absolutes Vetorecht des BR; in Betrieben ohne Betriebsrat braucht es dafür schriftliche Einzelzustimmungen aller betroffenen AN), (zweitens) Betriebsvereinbarungen über qualifizierte Personaldatensysteme (§ 96a Abs. 1 Z 1 ArbVG) und (drittens) Betriebsvereinbarungen über qualifizierte Mitarbeiterbeurteilungssysteme (§ 96a Abs. 1 Z 2 ArbVG). Diese Anwendungsfälle können sich auch (teilweise) überschneiden.

Mit dem zweiten Anwendungsfall sind Systeme zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des AN gemeint, die über die Ermittlung von allgemeinen Angaben zur Person (Generalien wie zB Name, Adresse, Geburtsdatum) und fachlichen Voraussetzungen (zB Ausbildungsweg, Befähigungsnachweise, bisherige berufliche Tätigkeiten) hinausgehen. Eine Zustimmung des BR ist (nur dann) nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben.

3.2. Verhältnis von Betriebsverfassung und Datenschutzrecht: Nebeneinander von zwei Ebenen

Nach bisheriger Rechtslage, vor allem aufgrund einer Leitentscheidung des österreichischen Obersten Gerichtshofes (OGH 17.09.2014, 6 ObA 1/14m) bestehen die Rechte, welche dem Betriebsrat nach ArbVG zustehen, und jene, welche das Datenschutzrecht den betroffenen einzelnen Mitarbeitern einräumt, nebeneinander.

An dieser Grundregel dürfte sich auch durch das neue Datenschutzrecht nichts geändert haben. Die auf die Verarbeitung personenbezogener Daten bezogenen Rechte des Betriebsrates nach ArbVG (3. Hauptstück) bleiben meiner Meinung nach unberührt, sie stehen neben den Individualrechten der AN als Betroffene nach Datenschutzrecht.

Mit anderen Worten: Die Zustimmung der Belegschaftsvertretung, die in Betrieben mit Betriebsrat für bestimmte Personaldaten-Verarbeitungen nach Betriebsverfassung nötig ist und in Form des Abschlusses einer entsprechenden Betriebsvereinbarung erteilt wird, ist kein Ersatz für die nach Datenschutzrecht allenfalls nötigen individuellen Zustimmungen (Einwilligungen) der einzelnen AN!

3.3. Grundsatz: keine Befugnisse des BR zur Durchsetzung von Datenschutz-Ansprüchen der AN

In einer Entscheidung zur früheren Rechtslage (OGH 29.06.2006, 6 ObA 1/06z) hat der Oberste Gerichtshof in Österreich entschieden, dass der BR im Normalfall nicht datenschutzrechtlich Betroffener ist und er daher auch nicht Betroffenenrechte nach dem Datenschutzrecht im Arbeitsverhältnis durchsetzen kann. Der BR kann also Ansprüche (Unterlassung, Beseitigung) „nur“ wegen Verletzung *seiner* betriebsverfassungsrechtlichen Mitbestimmungsrechte einfordern/einklagen, nicht mehr und nicht weniger.

An diesem Prinzip hat sich meines Erachtens auch durch das neue Datenschutzrecht nichts geän-

dert.

3.4. Betriebsvereinbarung als neuer (zusätzlicher) Erlaubnisgrund im Datenschutzrecht?

Diskutiert wird derzeit die offene Frage, ob Betriebsvereinbarungen zusätzlich zu den Erlaubnisgründen nach der DSGVO eigenständige (neue) datenschutzrechtliche Rechtfertigungstatbestände bilden können oder nicht. Soweit ich überblicke, wird diese Frage im Schrifttum aus verschiedenen Überlegungen überwiegend verneint. Für endgültige Klarheit kann nur eine Entscheidung des Europäischen Gerichtshofes (EuGH) irgendwann in der Zukunft sorgen.

Es ist jedenfalls zu empfehlen, sich bis auf Weiteres (nur) an den Kreis der Erlaubnistatbestände in der DSGVO zu halten und nicht neue in einer Betriebsvereinbarung zu kreieren.

3.5. Besteht ein Anpassungsbedarf für bestehende Betriebsvereinbarungen mit HR-Datenverarbeitungsbezug?

Nein, das ist kein Muss. Jedoch ist es ratsam, bestehende Betriebsvereinbarungen kritisch daraufhin durchzusehen, ob sie inhaltlich den neuen Datenschutz-Standards der DSGVO (noch) entsprechen. Nachdem sich diese ja nicht allzu sehr verändert haben und bei den Mitbestimmungsrechten des BR gar nichts neu ist, sollte hier (idealerweise) nicht allzu viel anzupassen sein. Auch könnten formale Anpassungen vorgenommen werden (zB Streichen bzw. Adaptierung von Verweisen auf das alte DSG 2000, Anführen der neuen Begrifflichkeiten in Klammer [Auftraggeber (Verantwortlicher)] etc.). Alte Betriebsvereinbarungen bleiben natürlich bestehen.

4. Datengeheimnis und Mitarbeiter

4.1. In aller Regel kommen nicht nur der Unternehmer selbst, sondern auch seine Mitarbeiter bei Ausübung ihres Jobs (berufsmäßige Beschäftigung) in Kontakt mit unterschiedlichsten personenbezogenen Daten (von Kunden, Lieferanten, anderen Mitarbeitern etc.). Schon nach bisheriger Rechtslage (§ 15 DSG 2000) war daher (auch) der Mitarbeiter als Träger des Datengeheimnisses zur Einhaltung desselben verpflichtet.

4.2. Die nunmehr gültigen Regelungen zum Datengeheimnis finden sich im § 6 DSG neu. Im Kern sind die dortigen Regelungen ident mit dem „alten" Datengeheimnis, es erfolgten im Grunde nur sprachliche Anpassungen (neue Begrifflichkeiten).

Nach aktueller (und auch schon früherer) Rechtslage muss der AG als datenschutzrechtlich Verantwortlicher (vormals „Auftraggeber") seine Mitarbeiter (echte AN und arbeitnehmerähnliche Personen) vertraglich verpflichten,

- das Datengeheimnis einzuhalten, und zwar nicht nur während des Arbeitsverhältnisses, sondern auch (explizit) nach dessen Beendigung,
- personenbezogene Daten aus Datenverarbeitungen nur aufgrund von ausdrücklichen Anordnungen des AG zu übermitteln („Auftragsprinzip") und
- die Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses belehren.

Eine Ausnahme von diesen Verpflichtungen besteht nur dann, wenn die Mitarbeiter bereits *von Gesetzes wegen* zur Verschwiegenheit verpflichtet sind. Diese Ausnahme wird bei der überwiegenden Zahl der Unternehmen in der Privatwirtschaft nicht greifen.

4.3. Es empfiehlt sich daher, bei bestehenden oder künftig neuen Mitarbeitern den Arbeitsvertrag um einen (eigenen, optisch hervorgehobenen) Datengeheimnis-Passus zu ergänzen oder die Mitarbeiter eigene Verpflichtungserklärungen unterfertigen zu lassen (Muster der Wirtschaftskammer Österreich auf www.wko.at/Datenschutz).

4.4. Eine vorsätzliche Datenübermittlung in Verletzung des Datengeheimnisses ist allein nach nationalem österreichischem Recht mit Geldstrafe bis zu € 50.000,-- bedroht (§ 62 Abs. 1 Z 2 DSG neu).

5. Datenschutzerklärung für Mitarbeiter

5.1. Geleitet vom Grundsatz der Transparenz sehen die Art. 13 und 14 DSGVO umfangreiche Informationspflichten des Verantwortlichen (hier: des AG) gegenüber den betroffenen Personen (hier: den AN) vor. Diese Informationen müssen dem Betroffenen zum Zeitpunkt der Erhebung der Daten (proaktiv/unaufgefordert) zur Verfügung gestellt werden.

Die Informationspflichten bestehen (nur) dann nicht, wenn die betroffene Person bereits über die Informationen verfügt oder die Informationserteilung unmöglich wäre bzw. einen unverhältnismäßigen Aufwand erfordern würde.

5.2. Es gibt unterschiedliche Möglichkeiten/Wege, den Informationspflichten nachzukommen. In der Praxis hat es sich als zweckmäßig und sinnvoll erwiesen, dies in Form von sog. Datenschutzerklärungen für bestimmte standardisierte Geschäftsbereiche zu machen. Angeraten wird daher eine eigene Datenschutzerklärung für die Mitarbeiter.

Diese spezielle Mitarbeiter-Datenschutzerklärung muss, nachdem sie bloß Informationszwecken dient, nicht unterschrieben oder sonstwie elektronisch (zB über eine Checkbox) bestätigt werden. Sie wird auch nicht Vertragsinhalt. Eine Bestätigung der Kenntnisnahme durch die AN schadet freilich nicht.

Die Mitarbeiter-Datenschutzerklärung kann/soll etwa auf leicht auffindbare Weise im Firmen-Intranet kundgemacht, am „Schwarzen Brett" angeschlagen und/oder auch als Papieranhang zum Arbeitsvertrag gegeben werden.

6. Kurzes zu Datenschutz-Dokumentationen aus HR-Sicht, Datenschutzbeauftragter

6.1. Verarbeitungsverzeichnis

Die Meldepflicht beim Datenverarbeitungsregister (DVR) ist weggefallen. Stattdessen müssen Unternehmen (AG) in Eigenverantwortung ein internes „Verzeichnis von Verarbeitungstätigkeiten" (Art. 30 DSGVO) mit den vorgegebenen Inhalten schriftlich oder elektronisch führen (Art „unternehmenseigenes DVR"). Dieses hat natürlich auch die verarbeiteten HR-Daten zu umfassen.

Von der Pflicht, ein Verarbeitungsverzeichnis zu haben, sind zwar Unternehmen mit weniger als 250 Mitarbeitern ausgenommen, doch gibt es beachtliche Ausnahmen von der Ausnahme. Die Pflicht besteht unter anderem dann wieder, wenn die Datenverarbeitung nicht nur gelegentlich erfolgt oder wenn besondere Datenkategorien (sensible Daten) verarbeitet werden. Eine dieser (alternativen) Ausnahmen von der Ausnahme ist in einem „gewöhnlichen" Unternehmen wohl immer erfüllt, allein schon deswegen, weil man es bei Mitarbeitern auch mit Krankenständen und deshalb mit sensiblen Gesundheitsdaten zu tun hat.

Auch der BR kann meines Erachtens vom AG Einsicht in dieses (interne) Verarbeitungsverzeichnis verlangen, weil sich sein Inhalt (Art. 30 DSGVO) im Wesentlichen mit dem Einsichtsrecht nach § 91 Abs. 2 ArbVG (siehe 3.1.) deckt.

6.2. Auftragsverarbeiterverträge

Als Unternehmen müssen Sie nicht mit allen Geschäftspartnern eine Auftragsvereinbarung (Art. 28 DSGVO) abschließen, sondern nur im Falle der Weitergabe personenbezogener Daten an einen Auftragsverarbeiter.

Typische Auftragsverarbeiter in der betrieblichen Praxis sind etwa: Externer Personalberater beim Recruiting, externe Buchhaltung, IT-Service-Provider, Anbieter von IT-Cloud-Lösungen oder etwa Software-Hersteller, die zu Wartungszwecken (Fernwartung) Zugriff auf die mit dem EDV-Tool verarbeiteten Daten (inklusive HR-Daten) haben.

Mit diesen Drittanbietern müssen Sie, auch wenn es sich dabei um in einer Unternehmensgruppe verbundene Unternehmen (Konzerngesellschaften) handeln sollte, DSGVO-konforme schriftliche Auftragsverarbeiterverträge („EU-Standardvertragsklauseln") abschließen. Verschaffen Sie sich also einen Überblick über alle Ihre Dienstleister/ausgelagerten Dienste (mit und ohne HR-Bezug)!

6.3. Datenschutz-Folgenabschätzung nötig?

Eine Datenschutz-Folgenabschätzung ist nicht immer nötig. Im Gegenteil: Die österreichische

Datenschutzbehörde hat in einer Art White-List (Verordnung über die Ausnahmen von der Datenschutz-Folgenabschätzung [DSFA-AV], BGBl II 2018/108) bestimmte Arten von Verarbeitungsvorgängen aufgelistet, für die (explizit) keine Datenschutz-Folgenabschätzung erforderlich ist. Als relevant in punkto Mitarbeiterdaten sind hier vor allem folgende Verarbeitungsvorgänge zu nennen:

> Personalverwaltung (DSFA-A02)
> Zutrittskontrollsysteme (DSFA-A08)
> stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung) (DSFA-A09)
> Bild- und Akustikdatenverarbeitung in Echtzeit oder zu Dokumentationszwecken (DSFA-A10 und DSFA-A11)

6.4. Achtung bei (Personal)Datenübermittlung ins EU/EWR-Ausland

Besondere Vorsicht ist bei der Übermittlung personenbezogener Daten (Personaldaten) ins EU/EWR-Ausland geboten.

Dies kann schnell einmal der Fall sein, denken Sie etwa an internationale Konzerne, wo Personaldaten im Konzern hin- und herfließen (Stichworte: internationale Personaldatenbanken, konzernübergreifende Personalverwaltungssysteme etc.) oder an Cloud-Provider, die außerhalb Europas sitzen und wo die Mitarbeiterdaten Ihrer Firma geparkt/behandelt werden.

Es bedarf hier eines angemessenen Schutzniveaus beim ausländischen Datenempfänger.

6.5. Datenschutzbeauftragter

Einen Datenschutzbeauftragten (Art. 37 DSGVO, § 5 DSG neu) benötigt es nur dann, wenn die Kerntätigkeit des Unternehmens (= Haupttätigkeit samt sämtlichen Schlüsseltätigkeiten, die untrennbar mit der Erreichung des Unternehmenszieles verknüpft sind; bloße Nebentätigkeiten wie etwa Personalverwaltung gehören nicht dazu) in der umfangreichen, regelmäßigen und systematischen Überwachung von betroffenen Personen besteht (zB beim Einsatz von Tracking, Scoring und Profiling etwa durch Banken oder Versicherungen) oder sensible oder strafrechtlich relevante Daten betrifft (trifft zu etwa bei Krankenhausgesellschaften und in der Pharmaindustrie). Andere Unternehmen brauchen also keinen Datenschutzbeauftragten.

Der Datenschutzbeauftragte kann, muss aber nicht ein Mitarbeiter des Unternehmens sein. Er agiert im Bereich des Datenschutzes unabhängig und weisungsfrei und unterliegt einer besonderen Verschwiegenheitspflicht.

7. Diverses zum Schluss: Hinweise, weitere Tipps, Empfehlungen

7.1. Die Videoüberwachung (vormals §§ 50a ff DSG 2000) ist nunmehr unter der neuen Begrifflichkeit „Bildverarbeitung“ (umfasst auch Fotos) in den §§ 12 f DSG neu geregelt. Unzulässig ist (weiterhin) die Bildbearbeitung (vormals Videoüberwachung) zum Zweck der Kontrolle von Arbeitnehmern.

7.2. Wenn Sie Mitarbeiterfotos auf der Firmen-Homepage oder auf Social-Media-Kanälen anbringen/nutzen wollen, holen Sie vorher in Datenschutzhinsicht entsprechende Einwilligungserklärungen der AN ein (daneben: Recht jedes AN am eigenen Bild nach § 78 UrhG). Die Berufung auf überwiegende berechtigte AG-Interessen dürfte eher nicht möglich sein.

7.3. Eine empfohlene TOM (= technische und organisatorische Sicherheitsmaßname): Erstellung einer internen Datenschutzrichtlinie, in welcher der Umgang mit personenbezogenen Daten für Ihre Firmenmitarbeiter verbindlich beschrieben wird (zB „Clean Desk Policy“).

7.4. Eine weitere empfohlene TOM: Schulen Sie Ihre Mitarbeiter regelmäßig unternehmensbezogen in Datenschutzbelangen und dokumentieren Sie diese Mitarbeiterschulungen. Vergessen Sie auch nicht auf die (stichprobenartige) Überwachung Ihrer Mitarbeiter!

7.5. Nach einer Empfehlung der sog. Art. 29-Datenschutzgruppe (neu vom 08.06.2017) sollte der AG – vor allem in Anwendung des Grundsatzes „privacy by default“ – darauf achten, dass bei Betriebsmitteln, die der AN für seine Arbeit erhält (zB trackingfähiges Dienst-Handy), immer die datenschutzfreundlichsten Voreinstellungen eingestellt sind.

7.6. Verwenden AN erlaubterweise ihre eigenen privaten Sachen (Smartphones, Notebooks oder Tablets) am Arbeitsplatz (BYOD: Bring Your Own Device) oder am Arbeitsplatz zuhause (Home-Office), sollte besonderes Augenmerk auf den Datenschutz gelegt werden.

7.7. Werden Betriebsmittel des AG auch für private Zwecke verwendet (zB cloud-basierter Kalender), ist eine Einschau des AG unzulässig, wenn Informationen als privat gekennzeichnet bzw. erkennbar sind. Das Verbot, Betriebsmittel für private Zwecke zu verwenden, ist arbeitsrechtlich zulässig und kann mitunter auch datenschutzrechtlich angezeigt sein.

7.8. Um die Nutzung bestimmter Internetseiten durch den AN für den privaten Gebrauch (bei teilweise erlaubter Privatnutzung) zu limitieren, empfiehlt die Art. 29-Datenschutzgruppe, bestimmte Internetseiten präventiv (technisch) zu blockieren.

7.9. Laut weiterer Empfehlung der Art. 29-Datenschutzgruppe sollten AG im Bewerbungsverfahren keinerlei Informationen über die Bewerber aus sozialen Netzwerken einholen. Ausnahmen sind Jobportale wie XING oder LinkedIn.

7.10. Eine Überwachung der genannten Jobportal-Profile ausgeschiedener Mitarbeiter wird dem AG für die Dauer eines etwaigen nachvertraglichen Wettbewerbsverbotes (Konkurrenzklausel) zugestanden, um die Einhaltung des legitimen AG-Interesses zu ermöglichen (weitere Empfehlung der Art. 29-Datenschutzgruppe).

7.11. Vermeiden Sie, gerade auch im HR-Bereich, „Ballast- bzw. Überschussdaten" (Grundsatz der Datenminimierung). Erforderliche Daten sind laufend aktuell zu halten („Up-date-Pflicht"). Sorgen Sie dafür, dass nur solche Personen in Ihrem Unternehmen Zugang zu Mitarbeiterdaten haben, die dies für ihre Arbeit auch tatsächlich brauchen (Personalabteilung, Geschäftsleitung, allenfalls nur noch Abteilungsleitung für die Abteilungsmitarbeiter).

7.12. Erstellen Sie nach Möglichkeit ein Löschkonzept für Mitarbeiterdaten! Personenbezogene Daten (also auch HR-Daten) müssen nämlich dann gelöscht werden, wenn der Zweck ihrer Verarbeitung entfallen ist und etwaige Aufbewahrungsfristen abgelaufen sind (Speicherbegrenzung).

Es gibt keine vorgeschriebenen bzw. fixen „Löschfristen", diese können je nach Konstellation, Datenart/en etc. unterschiedlich lang sein. Sie hängen vor allem auch von gesetzlichen Aufbewahrungsfristen, Anspruchs- und Klagsfristen etc. ab. Zur Illustration nur soviel:

Daten betreffend Lohnsteuer- und Abgabenpflicht sind 7 Jahre lang aufzubewahren (§ 132 Abs. 1 BAO). Daten betreffend Sozialversicherungsbeitragspflicht sind 3 bzw. 5 Jahre aufzubewahren (§ 68 ASVG). Arbeitsrechtliche Ansprüche verjähren grundsätzlich in 3 Jahren. Der Anspruch eines AN auf Ausstellung eines Dienstzeugnisses verjährt erst in 30 Jahren ab Beendigung des Arbeitsverhältnisses. Letzteres ist relevant für die Aufbewahrung der „Eckdaten" ausgeschiedener Mitarbeiter, bis ein Dienstzeugnis verlangt und ausgestellt wird.

Auf der Seite der Wirtschaftskammer Österreich (www.wko.at/service/.../eu-dsgvo-speicher-und-aufbewahrungsfristen.html) findet sich eine sehr hilfreiche Checkliste zu wichtigen (bundes)gesetzlichen Speicher- und Aufbewahrungsfristen, auch speziell mit Blickrichtung Arbeitsverhältnisse.

Es ließe sich noch viel zum Thema Mitarbeiter-Datenschutz nach neuem Datenschutzrecht sagen. Einiges ist ausgespart worden oder konnte bloß kurz gestreift werden. Ich hoffe dennoch, dass dieser kompakte Kurz-Überblick ein hilfreicher Einstieg und Arbeitsbehelf für alle „Personalisten" und sonstigen Akteure in der Privatwirtschaft ist, die mit Personaldaten im Unternehmen unmittelbar oder auch nur am Rande zu tun haben.

Aus Gründen der Lesbarkeit wird in dieser Broschüre darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Personenbezogene Formulierungen beziehen sich auf Frauen und Männer in gleicher Weise.

Ein Team von Spezialisten für fast alle Rechtsgebiete

Die Rechtsanwaltskanzlei Greiter Pegger Kofler & Partner geht auf Dr. Josef Greiter zurück, der im September 1897 seine Kanzlei eröffnete. Seit damals schenken uns Klienten ihr Vertrauen. Wir verstehen uns heute als modernes, aus der Tradition gewachsenes Dienstleistungsunternehmen, das Klienten mit einem Team von Spezialisten in fast allen Rechtsgebieten berät und vertritt.

Unser Team besteht aus ca. 35 Mitarbeiterinnen und Mitarbeitern, davon derzeit 11 Rechtsanwälten. Einer unserer Schwerpunkte ist das Wirtschaftsrecht, wobei wir auch international tätige Klienten betreuen.

Der Blick über die eigenen Grenzen ist für uns eine Selbstverständlichkeit. Wir verfügen daher über ein Netzwerk persönlicher Kontakte zu Anwälten in fast allen Ländern und korrespondieren in den vier Sprachen Deutsch, Englisch, Französisch und Italienisch. Unsere vielfältige Erfahrung und unser Wissen geben wir durch Vortragstätigkeiten, insbesondere an Hochschulen und Universitäten, weiter.

Greiter
Pegger
Kofler

Rechtsanwälte

Greiter Pegger Kofler & Partner
Rechtsanwälte

Maria-Theresien-Straße 24
6020 Innsbruck, Austria

Telefon: +43 512 57 18 11
Fax: +43 512 58 49 25

office@lawfirm.at
www.lawfirm.at