



HR-Daten im Fokus

Kaum ein Unternehmensbereich bearbeitet so viele sensible Personendaten wie das HR: Bewerbungsunterlagen, Gesundheitsdaten, Lohnabrechnungen, Leistungsbeurteilungen und andere Daten. Gleichzeitig zeigt die Praxis, dass gerade im Personalbereich datenschutzrechtliche Grundregeln häufig übersehen werden. E-Mail-Konten ausgetretener Mitarbeitender bleiben monatelang aktiv, Überwachungssoftware wird ohne klare Rechtsgrundlage eingesetzt, und Datenschutzerklärungen gegenüber Mitarbeitenden fehlen gänzlich oder sind lückenhaft. Die Risiken, die daraus entstehen, treffen nicht nur die HR-Abteilung, sondern das gesamte Unternehmen oder gar die Entscheidungsträger, finanziell, regulatorisch und reputationsmässig.

Diese Ausgabe behandelt vier Themen: den Zugriff auf E-Mail-Accounts ausgetretener Mitarbeitender, die Abgrenzung zwischen zulässiger Kontrolle und unzulässiger Mitarbeiterüberwachung, die gesetzlichen Mindestinhalte einer Datenschutzerklärung für Mitarbeitende sowie die datenschutzrechtlichen Fallstricke beim Outsourcing von HR-Prozessen wie Personaladministration und Payroll.

Entscheidsträger tragen die Verantwortung dafür, dass im Personalbereich datenschutzkonform gearbeitet wird. Diese Ausgabe liefert das nötige Rüstzeug.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre.

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

Outsourcing im HR – was ist aus datenschutzrechtlicher Sicht zu beachten?

Die Auslagerung von HR-Prozessen ist heute auch bei kleinen und mittleren Unternehmen weit verbreitet. Die externe Lohnbuchhaltung, cloudbasierte HR-Systeme, Bewerbungsplattformen oder externe Recruiting-Dienstleister können Prozesse vereinfachen und den Zugang zu spezialisiertem Know-how ermöglichen. Datenschutzrechtlich ist das HR-Outsourcing allerdings besonders sensibel: Personaldossiers enthalten regelmässig umfangreiche Informationen über Mitarbeitende und teilweise auch besonders schützenswerte Personendaten, beispielsweise Gesundheitsdaten.

■ Von Lukas Lezzi und Alexandra Egger

Besondere Anforderungen an die Bearbeitung von Personaldaten

Bei der Bearbeitung von Personaldaten sind neben dem DSG die besonderen arbeitsrechtlichen Vorgaben zu beachten. Art. 328b OR stellt eine Lex specialis zum DSG dar und erlaubt die Bearbeitung von Personaldaten nur, soweit sie die Eignung für das Arbeitsverhältnis betreffen oder für dessen Durchführung erforderlich sind. Dies gilt auch beim Outsourcing von HR-Prozessen: An externe Dienstleister dürfen grundsätzlich nur Personaldaten übermittelt werden, die der Arbeitgeber selbst rechtmässig bearbeiten darf.

Wann liegt eine Auftragsbearbeitung vor?

Eine Auftragsbearbeitung liegt vor, wenn ein externer Dienstleister Personendaten im Auftrag und nach den Weisungen des Verantwortlichen (Arbeitgebers) bearbeitet. Der Auftragsbearbeiter verfolgt mit der Bearbeitung keine eigenen Zwecke, sondern bearbeitet die Personendaten ausschliesslich für die vom Verantwortlichen festgelegten Zwecke.

Durch das Outsourcing wird die datenschutzrechtliche Verantwortung aber nicht auf den Dienstleister übertragen. Der Arbeitgeber bleibt als Verantwortlicher dafür zuständig, dass die Bearbeitung der Personaldaten datenschutzkonform erfolgt.

Wichtig zu beachten ist auch, dass die Wahrnehmung der HR-Funktion durch eine Gruppengesellschaft innerhalb eines Konzerns in vielen Fällen eine Auftragsbearbeitung darstellt.

Auswahl des Dienstleisters und Auftragsbearbeitungsvertrag

Nach Art. 9 DSG darf die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen werden, wenn dieser die Daten nur so bearbeitet, wie der Arbeitgeber selbst es tun dürfte, und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

Der Arbeitgeber muss sich zudem vergewissern, dass der Auftragsbearbeiter die Datensicherheit gewährleisten kann. Vor der Beauftragung sollten daher insbesondere die bearbeiteten



Personal­daten, die Bear­bei­tungs­orte, Zugriffs­be­rech­ti­gun­gen, Sicher­heits­mass­nah­men und der Ein­satz von Un­ter­auf­trags­bear­bei­tern ge­prüft wer­den.

Die Auf­trags­bear­bei­tung sollte in einem Auf­trags­bear­bei­tungs­ver­trag (ADV) ge­regelt wer­den. Das Schwei­zer DSG schrei­bt – an­ders als die DSGVO – kei­nen de­tail­lier­ten Ka­talog von Min­dest­be­stim­mun­gen vor. In der Praxis sol­len ins­be­son­dere Ge­gen­stand und Zweck der Bear­bei­tung, Da­ten­ka­te­go­rien, Wei­sungs­bin­dung, tech­ni­sche und or­ga­ni­sa­to­ri­sche Mass­nah­men (TOMs), Ver­traulich­keit, Kon­troll- und In­for­ma­tions­rechte, Mel­de­pflich­ten bei Ver­let­zun­gen der Da­ten­si­cher­heit, Un­ter­stüt­zungs­pflich­ten sowie Rück­ga­be oder Lös­chung der Da­ten ge­regelt wer­den.

Dabei ist ins­be­son­dere sicher­zu­stel­len, dass der Auf­trags­bear­bei­ter die Per­so­nen­da­ten nur für die verein­bar­ten Zwe­cke und ge­mäss den Wei­sun­gen des Ver­ant­wor­tl­ichen bear­bei­tet und sei­ne Mit­ar­bei­ten­den zur Ver­traulich­keit ver­pflich­tet sind. Dies ist bei be­son­ders schützens­wer­ten Per­so­nen­da­ten oder ge­setz­li­chen bzw. re­gu­la­to­ri­schen Ge­heim­hal­tungs­pflich­ten von be­son­derer Be­deu­tung. Angemes­sene Kon­troll­mög­lich­kei­ten könn­en etwa durch Au­dit­rechte, Zer­ti­fi­zie­run­gen oder un­ab­hän­gi­ge Au­dit­ber­ichte ge­währ­lei­stet wer­den.

Der Bei­zug von Un­ter­auf­trags­bear­bei­tern be­darf nach Art. 9 Abs. 3 DSG der vor­gän­gi­gen Ge­neh­mi­gung des

Ver­ant­wor­tl­ichen. In der Praxis wird dies häu­fig durch eine Liste ge­neh­mig­ter Un­ter­auf­trags­bear­bei­ter und ein Ver­fah­ren für spä­tere Än­de­run­gen um­ge­setzt.

Auch stan­dar­di­sierte und nur ein­ge­schränk­te ver­han­del­bare Ver­trä­ge gross­er Cloud- und HR-An­bie­ter sind sorg­fältig zu prü­fen. Ge­währ­lei­sten sie an­ge­sichts der aus­ge­lag­er­ten Per­so­nal­da­ten kei­nen aus­rei­chen­den Schutz und las­sen sich we­sen­ti­che Män­gel nicht be­heben, sollte von der Beauf­tra­gung ab­ge­se­hen wer­den.

Zugriff und Da­ten­si­cher­heit

Ge­rade bei HR-Da­ten ist ein re­stri­k­ti­ves Be­rech­ti­gungs­kon­zept zen­tral. Nicht sämt­liche Mit­ar­bei­ten­den des HR-Dienst­lei­sters dür­fen Zu­griff auf voll­stän­di­ge Per­so­nal­dos­si­ers er­hal­ten. Zu­griffe sol­len nach dem Need-to-know-Prin­zip auf die­je­ni­gen Per­so­nen be­schränk­te wer­den, die sie für ihre Auf­ga­ben tat­säch­lich be­nö­ti­gen.

Zu prü­fen sind fer­ner die tech­ni­schen und or­ga­ni­sa­to­ri­schen Mass­nah­men (TOMs) des Auf­trags­bear­bei­ters. Dazu ge­hö­ren be­spie­ls­wei­se Zu­griffs­kon­tröl­len, star­ke Au­then­ti­si­e­rung, Ver­schlüs­se­lung, Pro­to­kol­lie­rung, Back-up- und Wie­der­her­stel­lungs­ver­fah­ren sowie Pro­zes­se zur Be­han­dlung von Sicher­heits­vor­fäl­len. Je sen­si­bler und um­fang­rei­cher die aus­ge­lag­er­ten Da­ten sind, desto sorg­fältig­er sol­te die Prü­fung er­fol­gen. Zer­ti­fi­zie­run­gen und un­ab­hän­gi­ge Au­dit­ber­ichte könn­en dabei wich­ti­ge An­halt­spun­kte lie­fern.

Bei einer Ver­let­zung der Da­ten­si­cher­heit muss der Auf­trags­bear­bei­ter den Ar­bei­ter­ge­ber so rasch als mög­lich in­for­mie­ren. Ver­trag­lich sol­len kur­ze Mel­de­fris­ten (max. 48 h) sowie Mel­de­we­ge und die be­rei­tzus­tel­len­den In­for­ma­tio­nen fest­ge­legt wer­den, da­mit der Ar­bei­ter­ge­ber eine all­fäl­lige Mel­dung an den EDÖB bzw. In­for­ma­tion der be­trof­fe­nen Mit­ar­bei­ten­den beur­tei­len kann.

Trans­parenz ge­gen­über den Mit­ar­bei­ten­den

Auch bei aus­ge­lag­er­ten HR-Pro­zes­sen müs­sen die Grundsätze der Ver­hält­nis­mäs­sig­keit und Zweck­bin­dung ein­ge­hal­ten wer­den. Gleich­zei­tig ist eine an­ge­mes­sene In­for­ma­tion der Mit­ar­bei­ten­den zen­tral. Der Ar­bei­ter­ge­ber muss die In­for­ma­tions­pflich­ten nach Art. 19 DSG be­ach­ten und die Mit­ar­bei­ten­den ins­be­son­dere über die Bear­bei­tungs­zwe­cke, ihre Rechte im Zu­sam­men­hang mit der Bear­bei­tung ihrer Per­so­nen­da­ten sowie ge­ge­ben­falls die Em­pfän­ger oder Ka­te­go­rien von Em­pfän­gern in­for­mie­ren. Dies kann in einer Mit­ar­bei­ter-Da­ten­schutz-er­klä­rung er­fol­gen.

Beson­dere An­for­de­run­gen gel­ten, wenn HR-Da­ten ins Aus­land be­kannt ge­ge­ben wer­den. In die­sem Fall sind die Mit­ar­bei­ten­den ins­be­son­dere über den Em­pfän­ger­staat und – so­weit er­for­der­lich – über die ein­ge­setz­ten Ga­ran­ti­en für einen an­ge­mes­sene­n Da­ten­schutz zu in­for­mie­ren. Der EDÖB emp­fiehlt im Ar­beits­ver­hält­nis da­rüber hin­aus eine um­fas­sen­de In­for­ma­tion da­rüber, an wel­che Un­ter­neh­men die Da­ten über­mit­telt wer­den, wie diese im Aus­land bear­bei­tet wer­den und zu wel­chen Zwe­cken die Bear­bei­tung er­folgt.

HR-Da­ten im Aus­land

Be­fin­det sich ein Auf­trags­bear­bei­ter im Aus­land oder wer­den Per­so­nen­da­ten im Rah­men des Out­sour­cings ins Aus­land be­kannt ge­ge­ben, ist zu prü­fen, ob die Vor­aus­set­zun­gen des DSG für eine Aus­land­be­kannt­ga­be er­füllt sind. Bei Be­kannt­ga­ben in Staa­ten mit

einem angemessenen Datenschutzniveau, insbesondere in den EU-/ EWR-Raum, sind grundsätzlich keine zusätzlichen Garantien nach Art. 16 DSGVO erforderlich. Die entsprechenden Staaten sind in Anhang 1 der Datenschutzverordnung aufgeführt.

Bei Bekanntgaben in Staaten ohne angemessenes Datenschutzniveau sind geeignete Garantien erforderlich. In der Praxis werden hierfür insbesondere die gemäss dem DSGVO modifizierten EU-Standardvertragsklauseln (SCCs) eingesetzt. Zusätzlich ist zu prüfen, ob aufgrund der konkreten Umstände weitere Schutzmassnahmen, etwa eine Verschlüsselung der Personendaten, erforderlich sind.

Viele Outsourcing-Dienstleister haben ihren Sitz in den USA. Für Datenübermittlungen an US-Unternehmen kann ein angemessenes Datenschutzniveau vorliegen, sofern das betreffende Unternehmen unter dem Swiss-U.S. Data Privacy Framework zertifiziert ist.

Fazit

HR-Outsourcing entlastet Unternehmen administrativ, entbindet den Arbeitgeber jedoch nicht von seiner datenschutzrechtlichen Verantwortung. Gerade weil im Personalbereich umfangreiche und teilweise besonders schützenswerte Personendaten bear-

WICHTIGER HINWEIS

Red Flags bei der Auswahl eines HR-Dienstleisters

Bei der Auswahl eines HR-Dienstleisters kann insbesondere bei KMU eine kurze Red-Flag-Prüfung sinnvoll sein. Folgende Punkte können auf einen erhöhten Prüfungsbedarf hinweisen:

- **Datenschutzvorfälle:** Der Dienstleister war in der Vergangenheit von wesentlichen Verletzungen der Datensicherheit betroffen oder ist wiederholt durch Datenschutzvorfälle aufgefallen.
- **behördliche Verfahren:** Gegen den Dienstleister wurden wegen Datenschutzverstössen aufsichtsrechtliche Verfahren geführt oder Sanktionen verhängt.
- **fehlende Transparenz:** Der Dienstleister macht keine ausreichenden Angaben zu Bearbeitungsorten, Unterauftragsbearbeitern oder zum Umgang mit Personaldaten.
- **unzureichende Datenschutzorganisation:** Zuständigkeiten und Prozesse für Datenschutz, Datensicherheit und den Umgang mit Sicherheitsvorfällen sind nicht klar geregelt.
- **fehlende Nachweise:** Der Dienstleister kann keine geeigneten Nachweise über seine Datenschutz- und Sicherheitsmassnahmen, beispielsweise Zertifizierungen oder unabhängige Auditberichte, vorlegen.

beitet werden, sollten Dienstleister sorgfältig ausgewählt und die Datenbearbeitungen klar vertraglich geregelt werden.

Vor einer Auslagerung sollten Unternehmen insbesondere klären, welche Personaldaten für welche Zwecke ausgelagert werden, wer darauf zugreifen kann, welche Unterauftragsbearbeiter eingesetzt werden, in welchen Ländern die Daten bearbeitet werden und wie Vertraulichkeit, Datensicherheit, Betroffenenrechte sowie Löschung gewährleistet werden. Werden diese Punkte bereits bei der Auswahl und Vertragsgestaltung berücksichtigt,

lassen sich die Vorteile des HR-Outsourcings nutzen, ohne den Schutz der Personaldaten aus den Augen zu verlieren.

AUTOREN



Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.



Alexandra Egger arbeitet als Juristin bei LezziLegal. Sie arbeitet hauptsächlich im Bereich des Datenschutzes.

Inklusiv Seminargutschein im Wert von bis zu CHF 400.–

WEKA+ WEKA PRO WEKA PREMIUM

Jetzt WEKA MEMBER werden!

- | Zugriff auf alle kostenpflichtigen Beiträge und Videos
- | Unlimitierter Zugang zu allen Special Dossiers und über 1300 Arbeitshilfen
- | KI-Chatbot Evi: Das gesamte WEKA-Wissen mit Quellenangaben auf Abruf
- | Inkl. Zugang zu allen zweistündigen Live-Webinaren
- | Unlimitierte telefonische Rechtsberatung (PREMIUM)

Mehr Infos unter: www.weka.ch/member