Datenschutz im HR

Special Dossier

WEKA

Autorenteam

RA Dr. iur. Lukas Lezzi, CIPP/E, CIPM, CAS Forensics, ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Er hat in Zürich studiert und im Finanzmarktrecht dissertiert. Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

MLaw Alexandra Egger arbeitet als juristische Mitarbeiterin bei LezziLegal. Sie hat in Luzern studiert. Ihr Schwerpunkt liegt im Bereich Datenschutzrecht.

Priscilla Vallejo arbeitet als studentische Mitarbeiterin bei Lezzilegal. Sie studiert Rechtswissenschaften an der Universität Zürich.

MLaw Luciana Viganò arbeitet als juristische Mitarbeiterin bei LezziLegal. Sie hat an der Universität Zürich und Basel studiert. Ihr Schwerpunkt liegt im Bereich internationale Rechtsfragen.

Impressum

Datenschutz im HR

Special Dossier

Autorenteam Lukas Lezzi, Alexandra Egger, Priscilla Vallejo & Luciana Viganò

Projektleitung Tanja Pauly **Layout/Satz** Sarah Rutschmann **Korrektorat** Margit Bachfischer M.A., Bobingen

WEKA Business Media AG, Hermetschloostrasse 77, 8048 Zürich, Tel. 044 434 88 34
info@weka.ch, www.weka.ch, www.weka-library.ch

Zürich • Kissing • Paris • Wien

SD8125-2122-202512

Inhaltsverzeichnis

1 Einführung

In erster Linie sind die Arbeitgeber für den Datenschutz am Arbeitsplatz verantwortlich. Der vorliegende Leitfaden beleuchtet nicht nur die rechtlichen Aspekte des Datenschutzgesetzes (DSG), sondern hebt auch die Notwendigkeit hervor, den Datenschutz in die Unternehmens-Governance einzubeziehen.

Unternehmen müssen eine ganzheitliche Perspektive einnehmen und sämtliche relevanten Bereiche ihrer Governance-Struktur analysieren. In diesem Kontext erweist es sich als wichtig, die Wechselwirkungen zwischen dem DSG und anderen Unternehmensrichtlinien, Prozessen und Strukturen zu verstehen, weil das Thema Datenschutz in praktisch allen Aspekten eines Unternehmens zu berücksichtigen ist.

Das vorliegende Dossier gibt den Unternehmen einen praxisnahen Leitfaden an die Hand, um die Anforderungen des Datenschutzgesetzes im Bereich HR möglichst pragmatisch umzusetzen. Es werden die wichtigsten Punkte zur Umsetzung aus Sicht der Autoren besprochen, aber das DSG wird nicht gesamthaft kommentiert.

Damit es keine Missverständnisse gibt, folgen ein paar Definitionen:

a) **Personendaten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden «betroffene Person») beziehen, z. B. Name, E-Mail-Adresse, Gehaltsdaten, Telefonnummer (Art. 5 lit. a DSG).

b) **besonders schützenswerte Personendaten:** Diese bilden eine Unterkategorie der Personendaten. Alle folgenden Daten erfordern einen besonderen Schutz und eine strengere Handhabung (Art. 5 lit. c DSG):
   - Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder
   - Tätigkeiten
   - Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder
   - Ethnie
   - genetische Daten
   - biometrische Daten, die eine natürliche Person eindeutig identifizieren
   - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und
   - Daten über Massnahmen der sozialen Hilfe

c) **Bearbeitung:** Jeder Vorgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, z. B. Sammeln, Erfassen, Speichern, Verwenden, Ändern, Weitergeben, Löschen oder Vernichten von Personendaten (Art. 5 lit. d DSG).

d) **Verantwortlicher:** Eine natürliche oder juristische Person oder ein Bundesorgan entscheidet über den Zweck und die Mittel der Datenbearbeitung (Art. 5 lit. j DSG). Im Arbeitsverhältnis ist dies regelmässig der Arbeitgeber.

e) **Auftragsbearbeiter:** Eine natürliche oder juristische Person oder ein Bundesorgan, die Personendaten im Auftrag und auf Weisung des für die Bearbeitung Verantwortlichen bearbeitet. Der Auftragsbearbeiter hat keine eigenständige Entscheidungsbefugnisse über den Zweck und die wesentlichen Mittel der Datenbearbeitung (fehlendes Eigeninteresse). Ein Beispiel hierfür ist, wenn der Arbeitgeber (Verantwortlicher) einen externen Lohnabrechnungsdienstleister mit der monatlichen Gehaltsabrechnung beauftragt (Art. 5 lit. k DSG).

f) **Profiling:** Jede Form der automatisierten Bearbeitung von Personendaten zur Bewertung bestimmter persönlicher Aspekte, die sich auf eine natürliche Person beziehen, insbesondere zur Analyse oder Vorhersage von Aspekten (Art. 5 lit. f DSG). Ein Anwendungsbeispiel ist, wenn ein HR-Tool Log-in-Zeiten zählt und Statistiken für Team-Übersichten erstellt.

g) **Profiling mit hohem Risiko:** Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 5 lit. g DSG). Profiling mit hohem Risiko ist gegeben, wenn der Arbeitgeber eine Software zur Analyse der Arbeitsleistung einsetzt (z. B. Auswertung von Tastatureingaben, Log-in-Zeiten, Anzahl bearbeiteter Fälle) und daraus dann ein Performance-Score errechnet wird, der für Beförderungen oder Bonuszahlungen herangezogen wird. Hier handelt es sich um Profiling mit hohem Risiko, weil die automatisierte Bewertung unmittelbar wesentliche Aspekte der Persönlichkeit und beruflichen Zukunft betrifft.

2

Konkreter Umsetzungsprozess im Unternehmen

Es ist in jedem Fall für die Umsetzung des DSG empfehlenswert, im Unternehmen eine kleine Projektorganisation vorzusehen. Vorliegend wird der Fokus auf den Schutz der Mitarbeiterdaten gelegt. Diese Schritte können vom Unternehmen aber natürlich auch auf Kundendaten ausgeweitet werden. Grundsätzlich sollte in jedem Fall das Management eines Unternehmens als Stakeholder in einem solchen Projekt involviert sein. Als Unterstützung sollten in einem Projekt auch der interne Data Protection Officer (DPO) und Vertreter von Information Security mitwirken, sofern diese Funktionen vorhanden sind.

Generell empfiehlt es sich, bei der Umsetzung von einem solches Projekt Experten (z. B. durch Beauftragung einer Anwaltskanzlei oder eines Beratungsunternehmens) hinzuzuholen. Eine enge Zusammenarbeit von den Experten und dem Unternehmen ist essenziell, weil nach Abschluss des Projekts die neuen Prozesse auch tatsächlich intern akzeptiert und gelebt werden müssen. Dies kann nur erreicht werden, wenn die neuen Prozesse auch unternehmensintern erarbeitet werden. Ein Umsetzungsprojekt könnte sich wie folgt gliedern:

Workstream 1 – Data Mapping

In diesem Workstream werden die Datenflüsse und die Bearbeitungstätigkeiten von Mitarbeiterdaten analysiert. Weiter werden auch relevante Dienstleister und Verträge so identifiziert. Diese Arbeit ist die Voraussetzung für die weiteren Workstreams, kann aber auch für die initiale Erstellung eines Bearbeitungsverzeichnisses dienen.

Workstream 2 – Governance

In diesem Workstream werden die internen Weisungen und Prozesse definiert und festgelegt. Wichtige Aspekte im HR-Bereich sind:

- **Einhaltung der Mitarbeiterrechte:** Es ist festzulegen, wie die Rechte der Mitarbeitenden – wie Auskunftsrecht (Art. 25 DSG), Recht auf Datenherausgabe und -übertragung (Art. 28 DSG) – eingehalten werden können. Das heisst, es müssen Prozesse definiert werden, welche diese Rechte technisch und organisatorisch sicherstellen (z. B. Export aus HR-Systemen).
- **Umgang mit besonders schützenswerten Personendaten**: Besonders schützenswerte Personendaten dürfen nur unter strengen Voraussetzungen bearbeitet werden (Art. 5 lit. c DSG). Es müssen Guidelines erstellt werden, was bei der Bearbeitung von besonders schützenswerten Personendaten zu beachten ist.

– **Löschung/Aufbewahrung:** Es muss ein Löschungskonzept und eine Retention Policy eingeführt werden. Weiter müssen Prozesse definiert werden, welche sicherstellen, dass die Daten nach Austritt entsprechend gelöscht oder falls nötig archiviert und dann gelöscht werden.

Workstream 3 – Verträge und Datenschutzerklärungen

In diesem Workstream müssen Verträge und Datenschutzerklärungen angepasst bzw. neu erstellt werden. Zum einen müssen Mitarbeiter, ehemalige Mitarbeiter sowie Kandidaten über die Datenbearbeitung informiert werden, welche Daten wofür, wie lange, für welchen Zweck bearbeitet werden bzw. mit wem die Daten geteilt werden (Datenschutzerklärung). Zum anderen stehen im HR-Bereich Auftragsbearbeitungsverträge im Fokus. Typische Dienstleister im HR-Bereich, welche Mitarbeiterdaten bearbeiten, sind: Lohnbuchhaltung, Payroll-Provider, IT-Systeme (HR-Software, Cloud), Pensionskassen, Versicherungen, externe Recruiter.

Workstream 4 – Information-Security

Dieser Teil des Projekts deckt die Anforderungen an die Datensicherheit ab. Hier geht es darum, in einem ersten Schritt die konkreten Datensicherheitsmassnahmen zu definieren. Im HR-Bereich sind folgende Themen von zentraler Bedeutung:

– **Zugriffsbeschränkungen:** Es soll definiert werden, wer welche Personaldaten einsehen darf (z. B. dürfen Krankmeldungen nur für HR in vollem Detail ersichtlich sein).
– **Zugriffskontrollen:** Es soll überprüft werden, wer tatsächlich wann auf welche Mitarbeiterdaten zugegriffen hat.
– **besonders schützenswerte Daten:** sollen verschlüsselt werden

Workstream 5 – IT

In diesem Workstream werden die identifizierten Systeme auf gewisse für den Datenschutz relevante Funktionen analysiert. Hier fällt insbesondere die Erfüllung der Auskunfts- und Löschungsrechte und der Datenportabilität in Betracht.

Workstream 6 – Implementierung

In diesem abschliessenden Workstream werden insbesondere die neuen Prozesse implementiert, die Auftragsbearbeitungsverträge neu verhandelt, die Datenschutzerklärungen publiziert und die IT-Systeme angepasst. Die Anpassung von IT-Systemen hat in der Regel eine längere Vorlaufzeit, weshalb diese Implementierungsmassnahme zu priorisieren ist.

Workstream 1 und 2 können zuerst durchgeführt werden. Workstream 3 bis 5 hängen von 1 und 2 ab und können erst begonnen werden, nachdem die für diese Workstreams relevanten Themen in Workstream 1 und 2 abgeschlossen wurden. Workstream 6 erfolgt dann nachgelagert zu den vorgehenden Workstreams.

3

In welchen Etappen dürfen welche Daten bearbeitet werden?

3.1 Im Bewerbungsverfahren

Bewerbungsunterlagen dürfen ausschliesslich den Mitarbeitenden zugänglich gemacht werden, die direkt in den Bewerbungsprozess eingebunden sind. Im Bewerbungsverfahren soll der Arbeitgeber Informationen grundsätzlich direkt bei den Bewerbern einholen. Ist dies nicht möglich, dürfen Daten nur mit deren vorgängigem Einverständnis und bei klar definierten Dritten beschafft werden (Transparenzprinzip). Zudem müssen Personendaten richtig und vollständig sein.

Im Bewerbungsverfahren stehen der Schutz der Privatsphäre der Bewerbenden und das Informationsinteresse der Arbeitgeberin im Spannungsfeld. Grundsätzlich gilt:

- **Suchmaschinen und Personensuchdienste:** Recherchen über Google, Bing oder ähnliche Dienste sind unzulässig, da die Informationen oft unzuverlässig sind und Bewerbende keinen Einfluss auf deren Inhalt haben. Zudem besteht die Gefahr der Ungleichbehandlung bei häufigen bzw. seltenen Namen.
- **berufliche soziale Netzwerke:** Recherchen auf XING, LinkedIn und ähnlichen Plattformen sind erlaubt, da dort bewusst berufsbezogene Daten öffentlich zugänglich gemacht werden.
- **persönliche Webseiten, Blogs etc.:** Diese dürfen nur berücksichtigt werden, wenn die Bewerbenden von sich aus darauf hinweisen.

Grundsätzlich dürfen nur jene Daten bearbeitet werden, die für die Beurteilung der Eignung einer Person für die ausgeschriebene Stelle relevant sind. In folgenden Bereichen ist besondere Zurückhaltung geboten:

- **Strafregisterauszug:** Ein solcher darf in der Regel nicht verlangt werden. Meist genügt es, wenn sich der Arbeitgeber nach allfälligen relevanten Vorstrafen erkundigt. Ein Arbeitgeber darf nur dann einen Strafregisterauszug verlangen oder im Personaldossier aufbewahren, wenn dies objektiv für die konkrete Tätigkeit notwendig ist. Beispiele sind Tätigkeiten im Sicherheitsbereich (z. B. Flughafenpersonal, Polizei) oder auch Positionen mit hoher finanzieller Verantwortung (z. B. Bankwesen, Treuhand, Versicherungsvermittlung).
- **Gesundheitsfragen und Schwangerschaft:** Angaben zu bestehenden Krankheiten oder einer Schwangerschaft sind nur zulässig, sofern sie für die konkrete Stelle von Bedeutung sind – insbesondere dann, wenn eine gesundheitliche Gefährdung bestehen könnte. Eine mögliche Abwesenheit wegen Mutterschaftsurlaubs stellt hingegen keinen sachlichen

Grund dar. Auf Fragen, die für die Ausübung der Stelle nicht relevant sind, besteht keine Verpflichtung, wahrheitsgemäss zu antworten.

– **Referenzen und Auskünfte Dritter:** Informationen von ehemaligen Arbeitgebern oder anderen Dritten dürfen nur eingeholt werden, wenn der Bewerber dem ausdrücklich vorher zugestimmt hat.

Grundsätzlich müssen bei einer Absage alle Unterlagen zurückgegeben und allfällige Kopien vernichtet werden. Das gilt nicht für Unterlagen, die dem Arbeitgeber gehören (z. B. das Bewerbungsschreiben).

3.2 Während des Arbeitsverhältnisses

Personaldossier

Der Arbeitgeber sammelt die Daten, die für die Durchführung des Arbeitsverhältnisses notwendig sind, in einem sogenannten Personaldossier. Das Personaldossier enthält in der Regel folgende Informationen:

– Stammdaten (Name, Adresse, Geburtsdatum, Nationalität, AHV-Nummer, Zivilstand usw.)
– Vertragsunterlagen (Bewerbung, Lebenslauf, Arbeitsvertrag inkl. Anpassungen, Arbeitsbewilligung)
– Lohn- und Sozialversicherungsdaten (Bankverbindung, versicherungsrelevante Angaben)
– Leistungs- und Verhaltensdaten (Zielvereinbarungen, Mitarbeitergespräche, Beurteilungen, Weiterbildung, Absenzen, Disziplinarmassnahmen, relevante Korrespondenz)
– Arztzeugnisse
– Korrespondenz
– Aktennotizen

Die Bearbeitung von Personendaten von Mitarbeitenden richtet sich nach dem Art. 328b OR als Lex specialis zum DSG. Dieser Artikel geht dem DSG vor und besagt, dass die Personendaten von Mitarbeitenden nur so weit bearbeitet werden dürfen, wie dies für die Eignung oder für die Durchführung des Arbeitsverhältnisses erforderlich ist. Das heisst, dass bei jeder geplanten Datenbearbeitung, welche Personendaten von Mitarbeitenden betrifft, die Frage zu stellen ist, ob diese Bearbeitung tatsächlich für die Durchführung des Arbeitsverhältnisses erforderlich ist.

Die Bearbeitung der oben genannten Personendaten ist zulässig, da sie für die Durchführung des Arbeitsvertrags oder die Beurteilung der Eignung erforderlich ist. Unzulässig sind dagegen private Informationen ohne Bezug zur Arbeit (z. B. Freizeitgestaltung, familiäre Details) sowie ungeprüfte Gerüchte oder nicht belegte Beschwerden, da diese regelmässig unverhältnismässig und persönlichkeitsverletzend wären.