

## >> NEWSLETTER

### DATENSCHUTZ IM ARBEITSVERHÄLTNIS – WORAUF ALS ARBEIT- GEBER/IN ZU ACHTEN IST



MLAW SIMONE KESSLER  
RECHTSANWÄLTIN

[kessler@geissmannlegal.ch](mailto:kessler@geissmannlegal.ch)



MLAW KIM WYSSHAAR  
RECHTSANWÄLTIN

[wysshaar@geissmannlegal.ch](mailto:wysshaar@geissmannlegal.ch)

Am 1. September 2023 tritt das revidierte Datenschutzgesetz sowie die dazugehörige Verordnung in Kraft. Damit verbunden sind insbesondere auch weitergehende Pflichten der Arbeitgeberinnen und neue Rechte für Mitarbeitende. Der aktuelle Newsletter behandelt daher insbesondere die Anforderungen, welche an die Arbeitgeberinnen als Datenbearbeiterinnen gestellt werden, und welche Daten in welchen Fällen bearbeitet werden dürfen.

## I. ÜBERBLICK

In jedem Arbeitsverhältnis werden personenbezogene Daten der Mitarbeitenden bearbeitet. Dies beginnt in der Regel beim Bewerbungsprozess, indem die eingehenden Bewerbungsunterlagen abgespeichert werden. Während des laufenden Arbeitsverhältnisses werden die Personendaten der Mitarbeitenden im Rahmen der allgemeinen Personaladministration und der Lohnbuchhaltung verwendet und stetig aktualisiert. Auch nach Beendigung des Arbeitsverhältnisses werden die Daten der ausgetretenen Mitarbeitenden in der Regel nicht gleich gelöscht, sondern noch für eine gewisse Dauer aufbewahrt. Dabei handelt es sich stets um Datenbearbeitungen, die dem Schweizer Obligationenrecht und dem Datenschutzgesetz unterstehen.

Art. 328b OR bestimmt, dass die Arbeitgeberin Daten über Mitarbeitende nur bearbeiten darf, soweit sie deren Eignung für das Arbeitsverhältnis betreffen oder für die Durchführung des Arbeitsvertrages erforderlich sind. Gestützt auf das Datenschutzgesetz kann aber auch eine weitergehende Datenbearbeitung zulässig sein, wenn die betroffenen Mitarbeitenden explizit einwilligen oder die Arbeitgeberin oder ein Dritter ein überwiegendes Interesse daran hat (vgl. BGer 4A\_5118/2020).

Dies vorangestellt, wird nachfolgend auf einzelne Arbeitgeberpflichten im Zusammenhang mit der schweizerischen Datenschutzgesetzgebung eingegangen.

## II. INFORMATIONSPFLICHTEN

Sobald planmässig Personendaten bearbeitet werden, müssen die hiervon betroffenen Personen in der Regel vorgängig informiert werden – dies betrifft insbesondere auch Personendaten der eigenen Mitarbeitenden und Bewerbenden. Im Arbeitsverhältnis erfolgen diese Informationen in der Regel über ein Mitarbeiterreglement oder über eine interne Mitarbeiterinformation, welche den nachfolgenden Mindestinhalt aufweisen sollten:

- Wer ist für die Datenbearbeitung verantwortlich (inkl. Kontaktdaten)?
- Welche Daten werden erhoben?
- Weshalb werden diese Daten erhoben (Bearbeitungszweck)?
- Wem werden die erhobenen Daten weitergegeben?
- In welche Staaten können die Daten weitergegeben werden (Auslandsbekanntgabe) und gestützt auf welche rechtliche Grundlage?

Eine Ausnahme der Informationspflicht besteht hingegen dort, wo die Datenbeschaffung gesetzlich vorgeschrieben

ist. Gerade im Arbeitsverhältnis bestehen diverse gesetzliche Pflichten, die die Bearbeitung von Personendaten von Mitarbeitenden erfordern (zu denken ist bspw. an Meldepflichten im Zusammenhang mit Sozialversicherungen und der beruflichen Vorsorge, aber auch die Pflicht zur Ausstellung eines Arbeitszeugnisses bringt die Notwendigkeit mit sich, die Leistungen der Mitarbeitenden zu erfassen). Vor diesem Hintergrund besteht für Personendaten, die zur Erfüllung gesetzlicher Pflichten zwingend in einem Personaldossier geführt werden müssen, aller Voraussicht nach keine gesetzliche Informationspflicht.

Da die Qualifikation als "notwendige Daten" aber unter Umständen schwierig sein kann, empfiehlt sich dennoch eine proaktive Information durch die Arbeitgeberin. Denn wird in Verletzung der Informationspflicht nicht transparent über die Datenbearbeitung informiert, kann eine Verletzung der Persönlichkeitsrechte der betroffenen Mitarbeitenden oder Bewerbenden vorliegen. Die vorsätzliche Verletzung der Informationspflicht kann zudem mit Busse bis zu CHF 250'000.00 belegt werden.

## III. BEARBEITUNGSVERZEICHNIS

Für Unternehmen, die mind. 250 Mitarbeitende beschäftigen oder Daten bearbeiten, die ein hohes Risiko in sich bergen (bspw. umfassende Bearbeitung besonders schützenswerter Daten /Hochrisiko-Profiling), ist das Führen eines Datenbearbeitungsverzeichnisses Pflicht. Es soll der Nachvollziehbarkeit und Überprüfung sämtlicher Datenbearbeitungstätigkeiten dienen. Der Mindestinhalt wird durch Art. 12 revDSG festgelegt:

- Identität des Verantwortlichen
- Bearbeitungszweck

- Kategorien von betroffenen Personen und der bearbeiteten Personendaten<sup>1</sup>
- Aufbewahrungsdauer (hierzu nachfolgend)
- Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit
- Empfängerstaaten, falls die Personendaten ins Ausland gehen, sowie Garantien zum Datenschutzniveau der betroffenen Empfängerstaaten

Unternehmen, die weniger als 250 Beschäftigte haben und keine riskanten Datenbearbeitungen vornehmen, sind von dieser Pflicht hingegen ausgenommen.

---

<sup>1</sup> Als besonders schützenswerte Personendaten gelten Informationen zu religiösen, weltanschaulichen, politischen, gewerkschaftlichen Ansichten oder Tätigkeiten, Angaben zur Ethnie, Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen sowie genetische und biometrische Daten.

<sup>2</sup> Ein hohes Risiko liegt vor, wenn die Persönlichkeit / die Grundrechte der betroffenen Person besonders gefährdet sind, indem das Profiling zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt.

## IV. AUFBEWAHRUNGSDAUER

Das Datenschutzgesetz sieht keine maximale Aufbewahrungsdauer vor, sondern bestimmt lediglich, dass Personendaten grundsätzlich nur so lange bearbeitet und aufbewahrt werden dürfen, als dies für den Bearbeitungszweck notwendig, gerechtfertigt und verhältnismässig ist. Anschliessend müssen die Daten entweder anonymisiert oder gelöscht werden. Eine pauschale Aussage, wonach sämtliche Personendaten erst nach einer gewissen Anzahl Jahre gelöscht werden müssten, ist folglich nicht möglich. Vielmehr bedarf es einer

Einzelfallbeurteilung, wobei insbesondere gesetzliche Aufbewahrungspflichten und Verjährungsfristen berücksichtigt werden sollten. Allgemein festgehalten werden kann jedoch, dass eine Aufbewahrungsdauer von über 10 Jahren kaum zu rechtfertigen sein wird. Unterlagen von zurückgewiesenen Bewerbenden sind dahingegen unmittelbar zu retournieren oder zu löschen, sofern der Bewerber/die Bewerberin nicht explizit in eine längere Aufbewahrungsdauer eingewilligt hat (bspw. für potentielle andere in Zukunft entstehende Vakanzen).

## V. AUSKUNFTSRECHT

Während des laufenden Arbeitsverhältnisses hat jeder Mitarbeitende das Recht auf Auskunft über die eigenen Daten und insbesondere auf Einsicht in sein eigenes Personaldossier. Die Auskunft hat grundsätzlich kostenlos innert 30 Tagen zu erfolgen. Dabei zu beachten gilt, dass die Erteilung einer falschen oder unvollständigen Auskunft unter Strafanzeige steht (bei Vorsatz ebenfalls Busse bis zu CHF 250'000.00). Es sollte deshalb nicht der Eindruck erweckt werden, dass die Auskunft vollständig ist, geschweige denn eine Vollständigkeitserklärung abgegeben werden.

Das Auskunftsrecht gilt hingegen nicht absolut. Sprechen überwiegende Interessen Dritter oder eigene überwiegende Interessen (insbesondere Geschäftsgeheimnisse)

dagegen, kann die Auskunft verweigert werden. Gleiches gilt, wenn das Auskunftsbegehren offensichtlich unbegründet oder querulatorisch ist. Dies ist insbesondere dann der Fall, wenn das Gesuch einen datenschutzwidrigen Zweck verfolgt.

Nach Beendigung des Arbeitsverhältnisses bedarf das Auskunfts-gesuch grundsätzlich einer besonderen Rechtfertigung.

Ergänzend sei darauf hingewiesen, dass die Arbeitgeberin Dritten gegenüber nur Auskünfte erteilen darf, wenn der betroffene Mitarbeitende hiermit einverstanden ist. Ansonsten ist die Arbeitgeberin nicht dazu befugt, Auskunft über das Arbeitsverhältnis zu erteilen.

## VI. BERICHTIGUNGSRECHT

Die Arbeitgeberin darf über die Mitarbeitenden nur richtige Daten bearbeiten. Stellen Mitarbeitende fest, dass über sie falsche Daten erfasst wurden, haben sie ein Recht auf Berichtigung. Keiner Korrektur zugänglich sind allerdings rein subjektive Wertungen, da diese

schlichtweg nicht auf deren Richtigkeit überprüft werden können. Ist nicht klar, ob die erfassten Daten nun korrekt sind oder nicht, so ist zumindest ein entsprechender Vermerk anzubringen.

## VII. PROFILING – AUTOMATISIERTE EINZELENTSCHEIDE

Besondere Vorschriften gelten sodann, wenn gestützt auf erstellte Persönlichkeitsprofile automatisierte Einzelentscheide getroffen werden. Führt ein so getroffener Entscheid für die betroffene Person zu einer Rechtsfolge oder wird sie dadurch erheblich beeinträchtigt, muss sie vorgängig darüber informiert werden. Gleichzeitig hat die betroffene Person ein Recht auf Stellungnahme und sie kann verlangen, dass der Entscheid von einer natürlichen Person überprüft wird (sog.

Widerspruchsrecht). Klassisches Beispiel hierfür ist der Einsatz von Recruiting-Software, die eine Entscheidung vollautomatisiert auf der Basis einer durch Profiling erstellten Bewertung trifft.

Die vorgenannten Voraussetzungen gelten allerdings nicht, wenn die betroffene Person vorgängig explizit eingewilligt hat oder der Entscheid im Sinne der betroffenen Person ausgefallen ist.

## VIII. KONTROLLEN UND ÜBERWACHUNGEN AM ARBEITSPLATZ

Grundsätzlich ist die systematische Überwachung von Mitarbeitenden unzulässig (Art. 26 ArGV 3), da sie einen zu starken Eingriff in die Persönlichkeitsrechte der Mitarbeitenden darstellt. Werden im Betrieb dennoch Überwachungs- und Kontrollmassnahmen eingeführt, so bedarf es eines Rechtfertigungsgrundes (bspw. Sicherheitsgründe oder Leistungserfassung der Mitarbeitenden), wobei die ergriffenen Massnahmen auch in einem angemessenen Verhältnis zum angestrebten Zweck

stehen müssen. Die Mitarbeitenden sind vorgängig zu informieren. Werden Kontrollmassnahmen eingeführt, so sollten diese (verbunden mit der von der Arbeitgeberin erlassenen Weisung) in einem Reglement festgehalten werden. Klassisches Beispiel wäre der Erlass eines IT-Reglements, welches insbesondere die Leitplanken für die Nutzung von Internet und E-Mail sowie die diesbezüglichen Kontrollrechte der Arbeitgeberin festlegt.

## IX. PUBLIKATION VON FOTOS

Sollen Fotos von Mitarbeitenden publiziert werden – sei es im Intranet oder im Internet –, so bedarf es der expliziten vorgängigen Einwilligung der betroffenen Mitarbeitenden (Recht am eigenen Bild). Dies gilt auch für Fotos, die bei Veranstaltungen wie Apéros oder Betriebsausflügen gemacht werden. Aus der entsprechenden

Einwilligung sollten Art (Foto/Video/Tonaufnahmen etc.), Umfang (bspw. firmeneigene Website/Zeitschriften-Kolumne) und Zweck (bspw. zu Werbezwecken / Öffentlichkeitsarbeit) der Verwendung klar hervorgehen.

## X. BERUFSGEHEIMNIS

Abschliessend ist auf das mit der Datenschutzrevision neu einzuführende "kleine Berufsgeheimnis" hinzuweisen: Demnach müssen geheime Personendaten, die Mitarbeitende im Rahmen ihrer beruflichen Tätigkeit oder im Rahmen ihrer Ausbildung anvertraut wurden, geheim gehalten werden (bspw. eine Kundin klärt den Coiffeur

über ihre noch geheime Schwangerschaft auf, weil sie nicht jedes Haarfärbemittel verträgt). Wer vorsätzlich gegen das «kleine Berufsgeheimnis» verstösst, kann mit Busse bis zu CHF 250'000.00 bestraft werden. Es empfiehlt sich dringend, die Mitarbeitenden entsprechend für dieses Thema zu sensibilisieren.

15. August 2023 / MLaw Simone Kessler und MLaw Kim Wysshaar

---

GEISSMANN RECHTSANWÄLTE AG

MELLINGERSTRASSE 2A, FALKEN, POSTFACH, BADEN, TEL +41 56 203 00 11