Newsletter 01 | 2023

INHALTSÜBERSICHT

1. Datenschutz im Arbeitsverhältnis

1.1. Einleitung

Im Rahmen von Arbeitsverhältnissen erfasst und bearbeitet eine Arbeitgeberin eine Vielzahl von personenbezogenen Daten verschiedenster Art. Zusätzlich erlangt die Arbeitgeberin auch im Vorfeld eines Arbeitsverhältnisses, nämlich in Form von Bewerbungsunterlagen und Bewerbungsgesprächsinhalten, Kenntnis über sensible und personenbezogene Daten der Bewerber. Letztlich ist die Arbeitgeberin auch verpflichtet, gewisse Daten über einen längeren Zeitraum aufzubewahren, um den Anspruch auf Ausstellung eines wahren und aussagekräftigen Arbeitszeugnisses der ehemaligen Arbeitnehmer innert der Verjährungsfrist von 10 Jahren erfüllen zu können. Diesbezüglich stellen sich mannigfaltige Fragestellungen für eine Arbeitgeberin im Zusammenhang mit der Datenbeschaffung und -bearbeitung.

Nachfolgend werden die wichtigsten Grundsätze des Datenschutzes im Arbeitsverhältnis aufgezeigt und dargelegt, welche neuen Rechte und Pflichten das neu per 1. September 2023 in Kraft tretende revidierte Datenschutzgesetz mit sich bringt (abrufbar unter https://www.fedlex.admin.ch/eli/cc/2022/491/de).

Lars Müller

«Das revidierte Datenschutzgesetz tritt per 1. September 2023 in Kraft. Die neuen Regelungen haben auch für Arbeitgeber weitreichende Konsequenzen, derer sie sich nicht in jedem Fall bewusst zu sein scheinen.»

1.2. Gesetzliche Grundlagen

Gemäss Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im Übrigen gelten die Bestimmungen des Datenschutzgesetzes, ab 1. September 2023 in dessen revidierter Fassung.

Art. 328b OR gibt für das Arbeitsrecht wieder, was das revidierte Datenschutzgesetz bereits im Grundsatz regelt, nämlich, dass Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden und nur so bearbeitet werden dürfen, dass es mit diesem Zweck vereinbar ist (Art. 6 Abs. 3 revDSG).

1.3. Grundregel

Als Grundregel kann festgehalten werden, dass die Datenbearbeitung im Arbeitsverhältnis vorab durch die Zweckbindung in Art. 328b OR und Art. 6 Abs. 3 revDSG eingeschränkt wird. In ebendiesem Umfang ist die Datenbearbeitung aber im Grundsatz gesetzlich vorgeschrieben und damit rechtmässig. Für diese Datenbearbeitungen benötigt die Arbeitgeberin somit grundsätzlich keine (zusätzliche) Einwilligung der Arbeitnehmer oder einen anderen Rechtsfertigungsgrund für die Datenbearbeitung bzw. muss sie den Arbeitnehmer nicht über die Datenbearbeitung informieren (vgl. auch Art. 20 Abs. 1 Bst. b revDSG).

Die Datenbearbeitung einer Arbeitgeberin ist damit auch ohne Einwilligung und Information des Arbeitnehmers infolge gesetzlicher Pflicht insbesondere zulässig im Zusammenhang mit der Führung von Bewerbungsgesprächen, dem Abschluss des Arbeitsvertrages, der Auszahlung des

Lohnes, den Anmeldungen bei Sozialversicherungen, bei Weiterleitung von Arztzeugnissen an die Versicherungen, dem Führen des Personaldossiers sowie der Ausstellung von Arbeitszeugnissen etc.

Nur sofern eine Datenbearbeitung darüber hinaus geht, ist eine Einwilligung der Arbeitnehmer oder das Vorliegen eines anderen Rechtfertigungsgrundes für die Datenbearbeitung vorausgesetzt.

1.4. Einschränkung der Grundregel durch das Verhältnismässigkeitsprinzip

Die Grundregel wird u.a. durch das Verhältnismässigkeitsprinzip eingeschränkt: Jede Datenbearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig, d.h. notwendig für die Arbeitgeberin und zumutbar für den Arbeitnehmer sein (Art. 6 Abs. 2 revDSG). Die Arbeitgeberin hat dabei bei jeder Datenbearbeitung die Persönlichkeitsrechte des Arbeitnehmers zu wahren und sich an dessen berechtigten Interessen zu orientieren.

Obwohl durchaus argumentiert werden kann, dass Überwachungen am Arbeitsplatz mittels Video-, E-Mail- oder Telefonüberwachung zur Durchführung des Arbeitsverhältnisses erforderlich sein können, so sind gerade diese Datenerhebungen und -bearbeitungen infolge Beachtung des Verhältnismässigkeitsgrundsatzes nur unter eingeschränkten Bedingungen zulässig.

Dabei gilt zu beachten, dass die Arbeitnehmer ihre Einwilligung zu solch weitreichenden Massnahmen oftmals nur begrenzt rechtsgültig erklären können, da ihre Entscheidungsfreiheit durch das Subordinationsverhältnis zur Arbeitgeberin massgeblich eingeschränkt ist.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), welcher die Anwendung der bundesrechtlichen Datenschutzvorschriften beaufsichtigt (Art. 4 Abs. 1 revDSG), hat diesbezüglich klärende Erläuterungen und Leitfäden erarbeitet und erlassen (abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz.html).

1.5. Überwachungsmassnahmen am Arbeitsplatz

Einleitend und generell lässt sich sagen, dass es der Arbeitgeberin untersagt ist, das Verhalten der Arbeitnehmer mittels Überwachungsmassnahmen aufzuzeichnen. Dies wird bereits in Art. 26 Abs. 1 der Verordnung 3 zum Arbeitsgesetz festgehalten.

a) Videoüberwachung am Arbeitsplatz

Aus organisatorischen Gründen, aus Gründen der Sicherheit oder zur Produktionssteuerung können Videoüberwachungen zulässig sein. Es muss aber sichergestellt werden, dass die Arbeitnehmer nicht oder nur ausnahmsweise von der Kamera erfasst werden. Denkbar sind Videokameras ausserhalb der Gebäude und bei den Parkplätzen, bei Zugängen oder Eingängen, bei Durchgängen, bei gefährlichen Maschinen und Anlagen, in Tresorräumen, bei Gasinstallationen im Freien, bei Lagern mit gefährlichen oder wertvollen Gütern oder in der Schalterhalle einer Bank. Die Arbeitnehmer sind durch zweckmässige Information über die Überwachung zu informieren.

Die Aufbewahrung der Aufnahmen ist zeitlich zu begrenzen, wobei der jeweils verfolgte Zweck den Rahmen der Aufbewahrungsfrist vorgibt. Der EDÖB empfiehlt eine Löschung innert 24 – 72 Stunden.

b) Internet- und E-Mailnutzung

Das Verbot der Verhaltensüberwachung bedeutet in diesem Kontext für das Surfen und E-Mailen am Arbeitsplatz, dass das ständige personenbezogene Auswerten der Logdaten für die Überwachung des Nutzungsverhaltens der Arbeitnehmer nicht zulässig ist. Eingeschränkt wird dieses Prinzip hingegen für bestimmte Arten von Arbeitnehmern, wo aufgrund regulatorischer oder berufsspezifischer Compliance-Anforderungen eine Überwachung durch die Arbeitgeberin erforderlich sein kann (bspw. Banken).

Hingegen ist es erlaubt, das Surfen und E-Mailen personenbezogen auszuwerten, wenn mindestens ein konkreter Missbrauchsverdacht besteht.

Empfohlen wird, ein Nutzungsreglement für die private Nutzung des Internets und des E-Mails zu erlassen, damit die Arbeitnehmer wissen, was erlaubt und was verboten ist und sie bei einem konkreten Missbrauchsverdacht mit einer Auswertung der Daten rechnen müssen.

c) Telefonüberwachung

Die Arbeitgeberin ist nicht berechtigt, private Telefongespräche ihrer Arbeitnehmer abzuhören oder aufzunehmen. Eine solche Überwachung ist zur

Durchführung des Arbeitsvertrages nicht erforderlich. Die private Gesprächsüberwachung stellt eine Verletzung der Persönlichkeit dar und ist strafbewährt (Art. 179bis StGB).

Die geschäftliche Gesprächsüberwachung scheint hingegen zulässig zu sein, wenn sie der Beweissicherung und der Leistungskontrolle durch die Arbeitgeberin dient. Das Strafgesetzbuch setzt für eine rechtmässige Abhörung oder Aufnahme von Gesprächen die Einwilligung aller Gesprächsteilnehmenden voraus, weshalb sämtliche teilnehmenden Personen vor der Abhörung oder Aufnahme eindeutig und rechtzeitig in Kenntnis gesetzt werden und damit einverstanden sein müssen. Die vorherige Information verhindert auch die Aufnahme oder Abhörung privater Gespräche. Bei Arbeitnehmern kann diese Information im Arbeitsvertrag oder in einem Bestandteil davon erfolgen.

1.6. Informationspflichten

Bei jeder Datenbeschaffung ist die Arbeitgeberin verpflichtet – unter Ausnahme der gesetzlich vorgesehenen (Art. 20 Abs. 1 Bst. b revDSG) – aktiv über die Datenbeschaffung und -bearbeitung zu informieren. Dieser Pflicht kann mit einer Datenschutzerklärung gegenüber den Arbeitnehmern nachgekommen werden.

Der Mindestinhalt der Datenschutzerklärung ist in Art.19 revDSG geregelt, wobei insbesondere der Bearbeitungszweck sowie die Identität und die Kontaktdaten eines innerbetrieblichen Datenschutzverantwortlichen bekannt gegeben werden müssen.

Zu berücksichtigen ist letztlich, dass die Datenschutzerklärung jederzeit einseitig angepasst werden können sollte und aus diesem Grund in keinem Fall zum Bestandteil des Arbeitsvertrages erklärt werden sollte.

1.7. Verzeichnis sämtlicher Datenbearbeitungen

Das revDSG sieht eine Pflicht vor, ein Verzeichnis sämtlicher Datenbearbeitungen zu führen. Das Führen eines Datenbearbeitungsverzeichnisses wird für die meisten Arbeitgeberinnen mutmasslich zum grössten Aufwand bei der Umsetzung führen, falls nicht bereits entsprechende Massnahmen getroffen wurden. Der grosse Aufwand folgt daraus, dass sämtliche Datenbearbeitungen des gesamten Unternehmens erfasst und genaue Angaben dazu gemacht sowie laufend aktualisiert werden müssen. Der Mindestinhalt dieses Bearbeitungsverzeichnisses ist gesetzlich in Art. 12 revDSG vorgegeben.

Arbeitgeber, die am 1. Januar eines Jahres weniger als 250 Arbeitnehmer beschäftigen, sind grundsätzlich von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen (Art. 24 revDSV).

1.8. Auskunftsrecht

Die bereits bestehenden Auskunftsrechte nach bisherigem Datenschutzgesetz wurden zwar im Rahmen der Revision ausgebaut (Art. 25 ff. revDSG), aber gleichzeitig auch die Einschränkungsmöglichkeiten durch den Datenbearbeiter (hier interessierend: die Arbeitgeberin) erweitert.

Neu müssen auf Anfrage mehr Angaben als bisher geliefert werden, namentlich über (i) die Aufbewahrungsdauer, (ii) automatisierte Einzelentscheide und deren Logik sowie (iii) Angaben zu internationalen Übermittlungen.

Gleichzeitig wurden nebst den bisherigen Einschränkungen der (i) gesetzlichen Grundlage der Auskunftsverweigerung, (ii) überwiegenden Interessen Dritter, (iii) überwiegende eigene Interessen (z.B. Geschäftsgeheimnis), sofern die Daten nicht Dritten bekannt gegeben werden, neu auch (iv) die Einschränkung des offensichtlich unbegründeten oder querulatorischen Auskunftsbegehrens eingefügt (vgl. Art. 26 revDSG).

1.9. Korrekturrecht

Die von der Arbeitgeberin beschafften und bearbeiteten Daten müssen richtig sein und sie ist daher verpflichtet, durch angemessene Massnahmen sicherzustellen, dass die Daten in regelmässigen Abständen geprüft und gegebenenfalls aktualisiert werden (Art. 6 Abs. 5 revDSG).

Auf dieser Verpflichtung fusst auch der Rechtsanspruch der Arbeitnehmer, unrichtige Personendaten berichtigen zu lassen (Art. 32 Abs. 1 revDSG). In begründeten Fällen kann zudem durch ein Zivilgericht die weitere Datenbearbeitung verboten oder die Löschung angeordnet werden.

1.10. Datensicherheit

Die Datenbearbeitung ist technisch und organisatorisch so auszugestalten, dass unberechtigte Personen darauf nicht zugreifen können und die Datenschutzvorschriften eingehalten werden

(Art. 8 + 9 revDSG). Diese Vorgaben an die Datensicherheit dienen nicht nur dem Schutz vor unberechtigten Zugriffen von Aussenstehenden, sondern müssen auch innerhalb der Organisation der Arbeitgeberin so umgesetzt sein, dass nur die für die Datenbearbeitung zuständigen Personen auf diese zugreifen können. Der Kreis der berechtigten Personen ist so klein wie möglich, aber so gross wie notwendig zu halten.

1.11. Date Breach Notification und Datenschutz-Folgeabschätzungen

Verletzungen der Datensicherheit (z.B. Datenverluste, falsch adressierte E-Mails), die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der Arbeitnehmer führen, sind unverzüglich von der Arbeitgeberin dem EDÖB und gegebenenfalls dem betroffenen Arbeitnehmer zu melden.

Wenn eine beabsichtigte Datenbearbeitung oder eine Verletzung der Datensicherheit ein hohes Risiko einer Verletzung der Persönlichkeit oder der Grundrechte eines Arbeitnehmers mit sich bringt, ist die Arbeitgeberin zudem dazu verpflichtet, die Risiken einer solchen Bearbeitung bzw. Verletzung in einer Datenschutz-Folgeabschätzung zu analysieren. Nur so kann die Arbeitgeberin entscheiden, ob eine Meldung an den EDÖB zu erfolgen hat oder nicht.

1.12. Aufbewahrungsfristen

Gestützt auf diese allgemeinen Bearbeitungsgrundsätze dürfen Daten grundsätzlich nur so lange bearbeitet und aufbewahrt werden, als es für den Bearbeitungszweck notwendig und gerechtfertigt sowie verhältnismässig ist.

a) Bewerbungsunterlagen

Wird ein Bewerber oder eine Bewerberin abgelehnt, sind deren Daten grundsätzlich unverzüglich nach dem definitiven Entscheid der Nichtanstellung zu löschen. Unter Berücksichtigung von Art. 8 Gleichstellungsgesetz darf die maximale Aufbewahrungsfrist 3 Monate nicht übersteigen.

b) weitere Unterlagen / Personaldossier

Zumindest ein grosser Teil der Daten von (ehemaligen) Arbeitnehmern findet sich in dessen Personaldossier. Es stellt sich in jedem Einzelfall die Frage, welche Aufbewahrungspflicht für die Arbeitgeberin gilt und umgekehrt, welche Daten nach einer gewissen Zeit gelöscht werden müssen. Die jeweilige Aufbewahrungspflicht ist für die verschiedenen Arten der Daten separat zu ermitteln. Davon geht auch der EDÖB aus.

Klar scheint, dass geschäftsbuchrelevante Daten während zehn Jahren aufzubewahren sind (vgl. bspw. Art. 958f OR). Die weiteren Daten, welche im Zusammenhang mit finanziellen Forderungen der Arbeitnehmer mit Lohncharakter relevant sind, sind jedoch gemäss unserer Auffassung lediglich für fünf Jahre ab deren Fälligkeit aufzubewahren (siehe dazu Art. 128 Abs. 3 OR).

Der Anspruch eines Arbeitnehmers auf Ausstellung oder Berichtigung eines Arbeitszeugnisses verjährt zehn Jahre nach dem Ende des Arbeitsverhältnisses (Art. 127 OR). Entsprechend empfiehlt es sich aus unserer Sicht bzw. ist es gerechtfertigt, die im Zusammenhang mit dem Arbeitszeugnis relevanten Daten für zehn Jahre nach dem Ende des Arbeitsverhältnisses aufzubewahren.

Die Arbeitgeberin ist gut beraten, die von ihr erhobenen Daten periodisch zu überprüfen und sich mit der Frage auseinanderzusetzen, ob tatsächlich noch alle von ihr gespeicherten Daten aufbewahrt werden dürfen.

1.13. Verschärfung der Sanktionen

Das revDSG sieht strafrechtliche Sanktionen bei Verstössen gegen das revDSG in Form von Bussen von bis zu CHF 250'000 vor (Art. 60 ff. revDSG). Darüber hinaus kann der EDÖB ein verwaltungsrechtliches Untersuchungsverfahren eröffnen und Verfügungen erlassen. Auch wenn der EDÖB selbst keine Sanktionen anordnen kann, drohen auch bei Missachtung einer Anordnung des EDÖB, also bspw. bei der Weiterbearbeitung von Daten trotz Verbot, Strafsanktionen in der gleichen Höhe. Zuständig für die Durchsetzung der strafrechtlichen Sanktionen werden die kantonalen Strafverfolgungsbehörden sein.

2. Datenschutz im Mietverhältnis

2.1. Einleitung

Im mietrechtlichen Alltag stellen sich für Mieter, Vermieterinnen und Liegenschaftsverwaltungen immer wieder Fragen im Bereich des Datenschutzrechts. Das Bundesgesetz über den Datenschutz (DSG) wird per 1. September 2023 gewisse Neuerungen (revDSG) erfahren. Damit werden die datenschutzrechtlichen Anforderungen strenger, betroffen ist auch das Mietverhältnis. Nachfolgend werden die wichtigsten datenschutzrechtlichen Grundlagen aufgezeigt und anhand von Beispielen erläutert sowie die mit dem revDSG einhergehenden relevantesten Neuerungen zusammengefasst.

Irene Biber

«Die Bedeutung des Datenschutzes wird im mietrechtlichen Alltag häufig unterschätzt. Mit der per 1. September 2023 in Kraft tretenden Revision des Datenschutzgesetzes werden die datenschutzrechtlichen Anforderungen strenger. Betroffen davon sind Mieter, Vermieterinnen und Liegenschaftsverwaltungen.»

2.2. Grundsätze des Datenschutzrechts

2.2.1. Allgemeines

Das Datenschutzrecht gilt immer dann, wenn Personendaten bearbeitet werden, z.B. wenn solche Daten beschafft, gespeichert, bekanntgegeben oder gelöscht werden. Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, sind Personendaten. Das Datenschutzrecht verbietet die Bearbeitung von Personendaten nicht, fordert aber die Einhaltung bestimmter Grenzen. Konkretisiert werden diese Grenzen in den Bearbeitungsgrundsätzen. Liegen besondere Rechtfertigungsgründe vor, ist eine Verletzung der Bearbeitungsgrundsätze zulässig.

2.2.2. Bearbeitungsgrundsätze

a) Eidgenössischer Datenschutz- und Öffentlichkeitsberater (EDÖB)

Der Eidgenössische Datenschutz- und Öffentlichkeitsberater (EDÖB) hat Grundsätze betreffend Wohnungs- und Hausmiete veröffentlicht. Darunter finden sich auch wertvolle Angaben betreffend zulässige Auskünfte in Anmeldeformularen. (vgl. zum Ganzen Eidgenössischer Datenschutz- und Öffentlichkeitsberater (EDÖB), Erläuterungen zu den Anmeldeformularen für Mietwohnungen, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/wohnen-und-verkehr/Anmeldeformulare_Mietwohnungen.html).

b) Transparenzgrundsatz

Für die betroffenen Personen müssen zum Zeitpunkt der Beschaffung der Daten deren Beschaffung sowie der Zweck ihrer Bearbeitung erkennbar sein (Art. 4 Abs. 4 DSG, Art. 6 Abs. 3 revDSG). So ist es für Mietinteressenten ohne Weiteres erkennbar, dass ihre Angaben auf dem Anmeldeformular für die Miete eines Mietobjekts zum Zweck der Prüfung auf die Eignung als zukünftiger Mieter erhoben und bearbeitet werden.

c) Zweckbindungsgrundsatz

Die Bearbeitung der Personendaten darf nur zu dem Zweck erfolgen, der bei der Beschaffung der Personendaten erkennbar war oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG, Art. 6 Abs. 3 revDSG). So darf eine Liegenschaftsverwaltung die Angaben auf dem Anmeldeformular ohne entsprechenden Hinweis auf dem Formular nicht dazu verwenden, den Mietinteressenten über weitere mögliche Mietobjekte zu informieren.

d) Verhältnismässigkeitsgrundsatz

Die Vermieterin darf nur geeignete, notwendige und für den Mieter zumutbare Personendaten erheben. Häufig verletzen die in den Anmeldeformularen gestellten Fragen bereits diesen Grundsatz. Die abgefragten Daten müssen geeignet und notwendig sein, um den passenden Mieter zu bestimmen. Nicht geeignet hierzu und damit nicht verhältnismässig sind Fragen zum Zivilstand, zum Bürgerort und zur Konfession. Geeignet hingegen erscheint die Frage, ob jemand eine ausländische

Staatsangehörigkeit besitzt und über welche Aufenthaltsbewilligung der Mietinteressent verfügt und wann diese abläuft. Diese Auskunft ist notwendig für die Abschätzung, wie lange das Mietverhältnis dauern könnte. Eine nähere Bestimmung der ausländischen Staatsangehörigkeit erscheint hingen als nicht mehr zulässig.

Betreffend Angaben zum Einkommen ist mittlerweile anerkannt, dass nicht nach dessen exakter Höhe gefragt werden darf. Für die Beurteilung, ob der Mietinteressent als künftiger Mieter in Frage kommt, genügt es, ob er ein bestimmtes Jahreseinkommen erreicht oder in welchem Einkommensband sich sein durchschnittliches Jahreseinkommen bewegt.

Die Frage nach der Dauer des bisherigen Mietverhältnisses erscheint mangels Eignung als nicht zulässig. Die Dauer des bisherigen Mietverhältnisses hängt von verschiedenen Faktoren ab, sodass sie keinen zuverlässigen Schluss auf beispielsweise einen "Mietnomaden" zulässt. Hingegen ist es zulässig, zu fragen, ob das vorgängige Mietverhältnis durch die Vermieterin gekündigt worden ist und wenn ja, aus welchem Grund.

Ein Betreibungsregisterauszug darf erst vor Abschluss des Mietvertrages verlangt werden, nicht bereits als Teil der Anmeldung. Solche Vorgaben des EDÖB sind zwar verdienstvoll, in der Praxis jedoch nicht umsetzbar. Welcher Mietinteressent würde sich weigern, bei der Anmeldung einen Betreibungsregisterauszug vorzuweisen ohne Gefahr zu laufen, bereits bei der ersten Runde aus dem Rennen der Mietinteressenten auszuscheiden?

Schliesslich ist auch betreffend Aufbewahrungsdauer der Grundsatz der Verhältnismässigkeit zu wahren. Ist der Mietvertrag unterzeichnet, so sind die übrigen Bewerbungen zu vernichten.

e) Treu und Glauben / Rechtmässigkeit

In der Praxis ist dieser Grundsatz von untergeordneter Bedeutung. Zum Tragen käme er etwa, wenn die Vermieterin unwahre und ehrverletzende Referenzauskünfte über einen Mieter erteilen würde. Diesfalls würde die Vermieterin den Straftatbestand der üblen Nachrede oder der Verleumdung erfüllen und damit auch den datenschutzrechtlichen Grundsatz der Rechtmässigkeit verletzen.

f) Datensicherheit

Personendaten sind durch angemessene technische und organisatorische Massnahmen gegen unbefugte Bearbeitungen zu schützen (Art. 7 Abs. 1 DSG, Art. 8 revDSG). So hat eine Immobilienverwaltung ihre Mieterdatenbanken durch ausreichend komplexe Passwörter zu schützen und den Kreis der Berechtigten, welche Zugriff auf welche Daten haben, festzulegen. Der Zugang hat auf einer "need to know"-Basis stattzufinden.

2.2.3. Mögliche Rechtfertigungsgründe für die Missachtung eines Bearbeitungsgrundsatzes

a) Einwilligung

Die Einwilligung gilt dann als Rechtfertigungsgrund, wenn sie nach ausreichender Information freiwillig erfolgt (Art. 4 Abs. 5 DSG, Art. 6 Abs. 6 revDSG). Möchte also die Vermieterin beispielsweise einem Wohnungssuchenden inskünftig einen Newsletter mit Alternativangeboten zustellen, so kann der Wohnungssuchende dazu entsprechend seine Einwilligung erteilen.

b) Überwiegende private und öffentliche Interessen

Als Beispiel eines überwiegend privaten Interesses ist die Erfüllung des Mietvertrages zu nennen (allgemein die Erfüllung eines Vertrages: Art. 13 Abs. 2 lit. a DSG, Art. 31 Abs. 2 lit. a revDSG). So ist die Vermieterin beispielsweise berechtigt, einem Handwerker die Telefonnummer eines Mieters zwecks Vereinbarung eines Reparaturtermins bekanntzugeben.

c) Gesetzliche Bearbeitungsbefugnis

Die Vermieterin ist beispielsweise gesetzlich verpflichtet, der Gemeinde den Ein- und Auszug eines Mieters zu melden bzw. dessen Name, Vorname und Staatsangehörigkeit bekanntzugeben.

2.3. Revision des DSG

Das revDSG bezweckt einen besseren Schutz der Daten. Damit zusammenhängend erfährt das Gesetz gewisse Änderungen.

2.3.1. Datenschutzrechtliche Rollenverteilung

Neu aufgenommen im revDSG wurde das Begriffspaar "Verantwortlicher" sowie "Auftragsbearbeiter" (Art. 5 lit. j und k revDSG). Der Beizug ei-

nes Auftragsbearbeiters setzt eine Auftragsbearbeitungsvereinbarung voraus. Damit soll sichergestellt werden, dass der Auftragsbearbeiter den Weisungen des Verantwortlichen unterliegt und wichtige Pflichten zur Einhaltung des Datenschutzrechts beim Verantwortlichen bleiben.

Gemeinsam Verantwortliche sind für die Einhaltung des Datenschutzrechts gemeinsam verantwortlich. Ein Vertrag zwischen den gemeinsam Verantwortlichen ist zwar gesetzlich nicht vorgesehen, empfiehlt sich aber beispielsweise zur Abwehr von Haftungsrisiken bzw. zur Abgrenzung der jeweiligen Verantwortungsbereiche. Als Beispiel von gemeinsam Verantwortlichen ist zu nennen die Vermieterin und ihre Immobilienverwaltung.

2.3.2. Pflicht zur Führung eines Bearbeitungsverzeichnisses

Gemäss revDSG besteht die Pflicht zur Führung eines Verzeichnisses der Bearbeitungsgrundsätze (Art. 12 revDSG). Hierbei handelt es sich um eine generelle Beschreibung der einzelnen Kategorien von Bearbeitungstätigkeiten. Bei Immobilienverwaltungen sind hier typischerweise folgende Bearbeitungstätigkeiten zu nennen: Wohnungsbewerbungsmanagement, Vertragsabwicklung, Kommunikation mit Mietern, Stellenbewerbungsmanagement, Personaldatenverwaltung. Von der Pflicht ausgenommen sind KMU mit weniger als 250 Mitarbeitern und deren Datenbearbeitung nur ein geringes Risiko von Persönlichkeitsverletzungen der betroffenen Personen mit sich bringt.

2.3.3. Neue Informationspflicht

Neu ist eine eigenständige, aktive Informationspflicht bei der Datenbeschaffung vorgesehen, und zwar auch betreffend nicht besonders schützenswerte Personendaten (Art. 6 Abs. 3 revDSG). Offen ist allerdings, welche Informationen der Verantwortliche mindestens bekannt geben muss. Dies ist problematisch, da die Verletzung dieser Pflicht strafbewehrt ist (Art. 54 Abs. 1 lit. b DSG, Art. 29 StGB) Oft wird die Informationspflicht mit einer Datenschutzerklärung erfüllt; diese kann beispielsweise in das Anmeldeformular für Mietinteressenten und in den Mietvertrag integriert werden.

2.3.4. Rechte der Betroffenen

Zusätzlich zu dem bereits unter geltendem Recht bestehenden Auskunftsrecht haben die betroffenen Personen das Recht auf Berichtigung, zur Einschränkung der Bearbeitung, auf Vergessenwerden bzw. Löschung, das Widerspruchsrecht sowie das Recht, eine erteilte Einwilligung zu widerrufen (Art. 8 ff. DSG, Art. 24 ff. revDSG). Für das Mietverhältnis relevant ist das neu vorgesehene Recht auf Datenherausgabe und -übertragung. Ein Mieter kann damit beispielsweise kostenlos die Herausgabe seiner Personendaten in einem gängigen elektronischen Format verlangen.

2.3.5. Neue Meldepflicht

Neu sieht das revDSG vor, dass Verletzungen der Datensicherheit (nur der Datensicherheit, nicht der generellen Verletzung des Datenschutzes) dem Eidgenössischen Datenschutz- und Öffentlichkeitsberater (EDÖB) gemeldet werden müssen (Art. 24 revDSG). Eine Meldung ist dann erforderlich, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Der wohl häufigste Fall ist der Versand von E-Mails an eine falsche E-Mail-Adresse. Ferner ist an den Fall eines Hacker-Angriffs auf die Mieterdatenbank einer Liegenschaftsverwaltung zu denken. In jedem Fall ist eine Risikoabschätzung vorzunehmen unter Einbezug der Art der Verletzung, der Sensibilität und der Menge der betroffenen Daten, der Möglichkeit einer Identifizierung der betroffenen Personen, der Anzahl der betroffenen Personen, der Schwere der möglichen Auswirkungen für die betroffenen Personen und der Wahrscheinlichkeit der Risikorealisierung. Die entsprechenden Überlegungen und die getroffenen Massnahmen sollten dokumentiert werden. Erfordert es der Schutz der betroffenen Personen, müssen auch diese informiert werden. Zu denken ist etwa an den Fall, dass Unberechtigte Zugriff auf Bank- oder Kreditkarteninformationen erhalten.

3. Datenschutzrechtliche Risiken von Unternehmen

3.1. Daten als Ziel von Angriffen

Jeder und jede arbeitet mit Daten. Der Arbeitgeber bearbeitet Daten seines Personals. Die Vermieterin bearbeitet Daten ihrer Mieter. Der Unternehmer bearbeitet Daten seiner Kunden. Diese Daten können mehr oder weniger sensibel sein. Beim Arbeitgeber fallen z.B. sensible Daten zu Lohn, Bankverbindungen und Krankheiten der Arbeitnehmer an, bei einer Arztpraxis Daten zu Krankheiten und Behandlungen der Patienten, bei einem Treuhänder zu den finanziellen Verhältnissen der Klienten.

Martin Kern

«Datenschutz ist mehr als nur das Installieren eines Cookie-Popups auf der eigenen Website. Es geht um den Schutz des Unternehmens und der von ihm bearbeiteten Daten vor Angriffen, die im schlimmsten Fall das Unternehmen in existenzielle Nöte bringen können.»

Daten sind wertvoll. Sie sind oft die wesentliche Ressource, die es dem Unternehmer erlaubt, seine Dienstleistungen zu erbringen. Sie sind aber auch für diejenige Person wertvoll, von der sie stammen, also dem Kunden, Patienten, Arbeitnehmer und Mieter. Diese Personen sind meistens vor allem daran interessiert, dass ihre Daten nicht für alle frei zugänglich sind und sorgfältig behandelt werden.

Wertvolle Daten locken immer auch Übeltäter an, die selber daraus einen Nutzen ziehen wollen. Schon lange bekannt ist die Industriespionage, bei der Unternehmen ausgekundschaftet werden, um an vertrauliche Daten zu gelangen, die der Täter sich anschliessend selber zu Nutze machen kann.

Eher jüngeren Datums sind Angriffe aus dem Internet auf Daten, mit denen sich ein Täter indirekt einen Vorteil verschaffen will.

Zum einen versuchen Hacker, Zugriff auf ein Datensystem zu erhalten und dieses zu kidnappen, indem sie den Zugang darauf verschlüsseln und (vielleicht) erst wieder freigeben, nachdem ein Lösegeld (meist in Form von Bitcoin) bezahlt worden ist. Solange die Blockade andauert, ist das betroffene Unternehmen gehindert, seiner Geschäftstätigkeit normal nachzugehen. Je nachdem wie zuverlässig Backups vorhanden sind, kann die Wiederaufnahme des Geschäftsbetriebs länger oder kürzer dauern. Mit diesem erzwungenen Betriebsstopp gehen natürlich Umsatz- und Reputationsverluste einher.

Zum anderen versuchen Hacker, Zugriff auf ein Datensystem zu erhalten und die Daten zu kopieren. Anschliessend wird damit gedroht, dass die Daten im Internet veröffentlich werden, wenn nicht ein Lösegeld bezahlt wird. Je nach Art der Daten können die Konsequenzen für die Betroffenen mehr oder weniger schwerwiegend sein.

Die beiden Vorgehensweisen – Verschlüsselung des Systems und Androhung der Datenveröffentlichung – werden oft auch miteinander kombiniert.

3.2. Folgen eines erfolgreichen Angriffs

Sind nur die eigenen Daten eines Unternehmens betroffen, ist das Ganze ärgerlich und wirkt sich allenfalls finanziell aus, betroffen sind aber nur die eigenen Interessen. Sind aber Daten Dritter – eben bspw. von Klienten, Patienten, Personal, Mietern des Unternehmens – betroffen, dann wirkt sich das Verhalten des datenbearbeitenden Unternehmens auf Dritte aus, allenfalls mit erheblichen negativen Auswirkungen auf diese. Die betroffenen Dritten sehen sich bei einer Datenveröffentlichung möglicherweise damit konfrontiert, dass ihre vertraulichen Informationen allgemein zugänglich geworden sind. Im Falle einer Verschlüsselung sind sie vielleicht vom weiteren Leistungsbezug ausgeschlossen, was bei einer verzögerten Lieferung ärgerlich, aber meist nicht besonders schwerwiegend ist, im Falle verschlüsselter Patientendaten aber möglicherweise sogar gesundheitsgefährdend sein kann.

Wer im Zusammenhang mit seiner Leistungserbringung Daten Dritter sammelt und bearbeitet,

hat daher das Risiko, dass im Falle einer solchen Datenbeeinträchtigung finanzielle Ersatzforderungen von den betroffenen Dritten auf ihn zukommen. Datenschutz ist deshalb nicht einfach ein weiteres administratives Erschwernis für die Geschäftstätigkeit, sondern ein unbedingt zu berücksichtigender Risikofaktor. Eine risikobasierte Würdigung führt je nach Unternehmen zu unterschiedlichen Risikoeinschätzungen. Das Schreinerunternehmen, dessen Kundenkartei gehackt wird, hat ein geringeres Risiko als die Onkologiepraxis, deren Patientendossiers angegriffen werden. Es geht aber in allen Fällen darum, ein Bewusstsein dafür zu bekommen, was für Datenschutzrisiken mit der eigenen Geschäftstätigkeit verbunden sind.

3.3. Massnahmen gegen Datenschutzverletzungen

Abhängig von der Risikoeinschätzung sind anschliessend diejenigen Massnahmen umzusetzen, mit denen eine Datenbeeinträchtigung verhindert werden soll. Abhängig vom mit der Datenbearbeitung verbundenen Risiko können diese Massnahmen mehr oder weniger umfangreich sein. Offensichtlich erster Schritt ist die Umsetzung der nötigen technischen Infrastruktur (Hard- und Software). Nicht vergessen werden darf, dass es aber meistens der menschliche Faktor ist, der ein Unternehmen verletzlich macht: Mitarbeiter, die auf verdächtige Links klicken, vermeintlich legitime Instruktionen ausführen oder scheinbar zulässige Anfragen beantworten. Die Sicherheitsmassnahmen haben daher immer auch beim Personal durch Schulung und Sensibilisierung anzusetzen.

Zu beachten ist vor allem auch, dass Datenschutzverletzungen gar nicht irgendeinen bösen Willen voraussetzen: Ein unbeabsichtigter E-Mail-Fehlläufer mit Kundendaten kann bereits eine relevante Datenschutzverletzung darstellen, die Folgen nach sich ziehen kann.

Für den Fall, dass es zu einer Datenbeeinträchtigung kommt, sollte auch bereits ein Drehbuch vorliegen, was zu unternehmen ist. Dabei geht es um die Festlegung, was für Sofortmassnahmen zu ergreifen sind, welche Personen wofür zuständig sind, welche externen Akteure informiert / beigezogen werden sollen.

Je nachdem ist die Versicherungssituation daraufhin zu prüfen, ob eine Versicherung von Cyberrisiken sinnvoll ist.

3.4. Datenschutzgesetzgebung: national und international

Zur Schilderung der Datenschutzproblematik war es bis zu diesem Absatz noch nicht einmal nötig, die Datenschutzgesetzgebung zu bemühen. Diese ist aber immer auch anwendbar und deshalb zu beachten. Sie konkretisiert die oben bereits ausgearbeiteten Punkte weiter, legt aber auch weitere zu beachtende Pflichten fest. Dazu gehören insbesondere Pflichten gegenüber den Personen, deren Daten erhoben und bearbeitet werden, sowie Pflichten im Umgang mit der Bearbeitung von Daten. Hinzu kommen unter bestimmten Umständen auch Meldepflichten im Falle einer Datenbeeinträchtigung. Das Schweizer Datenschutzgesetz (DSG) wurde kürzlich revidiert und die neue Fassung wird am 1. September 2023 in Kraft treten. Bereits vorhandene Datenschutzvorkehrungen sollten daher dahingehend überprüft werden, ob sie auch dem neuen Recht genügen.

Weitet man den Horizont, erscheint auch bald einmal die europäische Datenschutzgesetzgebung in Form der DSGVO. Wer als Schweizer Unternehmen seine Dienstleistungen auch im europäischen Raum erbringt oder zumindest gewisse darauf ausgerichtete Handlungen unternimmt, muss diese Bestimmungen beachten. Die DSGVO sieht tendenziell schärfere Regelungen und Sanktionen vor als das Schweizer DSG.

3.5. Aufbau einer datenschutzbezogenen Sicherheitskultur

Alles in allem ist festzustellen, dass datenbezogene Angriffe immer raffinierter werden. Es hat sich eine eigentliche Industrie entwickelt, deren Zweck es ist, Unternehmen Lösegeld abzupressen. Je wesentlicher Daten für die Geschäftstätigkeit des Unternehmens sind, umso schwerwiegender ist ein erfolgreicher Angriff, sowohl für das Unternehmen als auch für die Personen, deren Daten betroffen sind. Für das angegriffene Unternehmen und seine Organe können sich aus Vernachlässigung ihrer Sorgfaltspflichten Haftungsfragen ergeben.

Aber auch der ganz normale Umgang mit Daten setzt die Beachtung der anwendbaren Datenschutzgesetzgebung voraus. Gewisse Verletzungen von Vorschriften können Sanktionen und ebenfalls Haftungsfolgen auslösen.

Alle diese Konsequenzen lassen sich nicht so leicht und unbesehen wegklicken wie die Cookie-

Popups im Internet, die wir ebenfalls der Datenschutzgesetzgebung zu verdanken haben. Im Gegenteil, diese Folgen sollten Anlass dafür sein, sich die eigenen Datenschutzrisiken bewusst zu machen und angemessenen Massnahmen zu ergreifen, um die Risiken soweit wie möglich zu minimieren. Ziel sollte der Aufbau einer datenschutzbezogenen Sicherheitskultur sein.

4. In eigener Sache

4.1. Anwalts-Ranking 2023: Erneut erfolgreich!

Wir freuen uns ausserordentlich, dass wir im jährlichen Anwalts-Ranking der BILANZ auch dieses Jahr wieder zu den Top-Kanzleien gehören. Im Bereich Compliance belegen wir schweizweit den ersten Platz, im Bereich Mietrecht gehören wir zur Top-Kategorie. Wie bedanken uns herzlich bei unseren Klientinnen und Klienten, die uns immer wieder ihr Vertrauen schenken und damit dazu beitragen, dass wir uns jahraus, jahrein in unseren Fachbereichen bewähren dürfen.

4.2. LinkedIn

Follow us on LinkedIn

Lutz Partner Rechtsanwälte AG
Tödistrasse 53
Postfach 1905
8027 Zürich

T +41 44 368 50 50

5. Team

Dr. Peter Lutz, LL.M.

Dr. Irene Biber

Martin Kern, M.A. HSG

Lars Müller, MLaw