BÄR & KARRER

BRIEFING SEPTEMBER 2023

PRAKTISCHE HINWEISE FÜR DIE UMSETZUNG DES REVIDIERTEN DATENSCHUTZGESETZES IM ARBEITSVERHÄLTNIS

Heute treten das neue Datenschutzgesetz (DSG) sowie die dazugehörige Verordnung (DSV) in Kraft. Die revidierten Datenschutzbestimmungen auferlegen Arbeitgebern neben den bisherigen eine Reihe neuer Pflichten. Diese neuen Pflichten müssen Arbeitgeber bereits ab Inkrafttreten einhalten, da für die Umsetzung der neuen Erlasse keine Übergangsfrist gilt. Bei Verletzungen von bestimmten Pflichten drohen neuerdings zudem höhere Individualbussen (bis zu CHF 250'000) als bisher.

Dieses Briefing dient Arbeitgebern als praktische Hilfestellung, um die neu auferlegten Pflichten im Rahmen des Arbeitsverhältnisses einzuhalten. Wir haben hier aber nur die wichtigsten für Arbeitgeber relevanten Neuerungen unter dem revidierten DSG dargestellt. Allfällige übrigen Rechte und Pflichten des bisherigen Datenschutzgesetzes gelten grundsätzlich unverändert weiter. Insbesondere besteht nach wie vor das Auskunftsrecht für Mitarbeitende, welches oft keine unbedeutende Rolle im Arbeitsverhältnis spielt.

INFORMATIONSPFLICHTEN

Arbeitgeber müssen ihre Mitarbeitenden neu über jede Erhebung und Bearbeitung von Personendaten informieren. Die Informationen, die zwingend bereitgestellt werden müssen, sind weniger umfassend als in der EU-Datenschutzgrundverordnung (EU-DSGVO). Gemäss DSG sind dies: die Identität des für die Bearbeitung Verantwortlichen, der Zweck der Bearbeitung, die Empfänger der Daten und die Kategorien von Daten, Übermittlungen von Daten ins Ausland, der Einsatz von automatisierten Einzelentscheiden (z.B., wenn ein Bewerbungstool eingesetzt wird, das Bewerbungen automatisch ohne menschliches Zutun ablehnt), Kontaktangaben des Schweizer Vertreters und des Datenschutzberaters. Im Gegensatz zur EU-DSGVO müssen die Mitarbeitenden zusätzlich noch über alle Datenempfängerländer und Schutzmassnahmen informiert werden, wenn Arbeitgeber Mitarbeiterdaten ins Ausland übermitteln.

Ausnahmsweise besteht keine Informationspflicht. Dies ist bspw. der Fall, wenn die Mitarbeitenden bereits über die entsprechenden Informationen verfügen, die Information den Zweck der Bearbeitung vereiteln würden (bspw. im Rahmen von internen Untersuchungen bei Kollusionsgefahr) oder überwiegende Drittinteressen dagegensprechen (bspw. die Wahrung von Geschäftsgeheimnissen oder der Schutz der Persönlichkeit einer anderen Person).

Wichtig ist in jedem Fall, dass Mitarbeitende über die Bearbeitung ihrer Daten im Rahmen interner Verfahren (oder auch Gerichtsverfahren) informiert werden.

Wer die Informationspflicht als Vorgesetzter vorsätzlich verletzt, kann persönlich gebüsst werden.

HANDLUNGSEMPFEHLUNG

Wir empfehlen den Arbeitgebern deshalb, spezifische Datenschutzerklärungen für Mitarbeitende einzuführen bzw. bereits bestehende zu überarbeiten. Alternativ können die Informationen auch in einem Mitarbeiterhandbuch integriert werden.

Eine Zustimmung der Mitarbeitenden zur Datenschutzerklärung oder zu den Informationen im Mitarbeiterhandbuch ist grundsätzlich nicht notwendig.

Zudem ist zu beachten, dass die Informationspflicht auch gegenüber Stellenbewerbenden gilt, deren Personendaten im Bewerbungsprozess naturgemäss bearbeitet werden. Wir empfehlen bspw. für Online-Bewerbungen eine entsprechende Datenschutzerklärung bereits auf der Website einzubauen oder im Antwortschreiben auf die Bewerbung auf die Datenschutzerklärung zu verweisen. Auch über eine allfällige Nutzung von auf künstlicher Intelligenz beruhender Software im Bewerbungsverfahren müssen die Stellenbewerbenden aufgeklärt werden.

AUSLAGERUNG VON DATENBEARBEITUNGSTÄTIGKEITEN

Die Pflichten betreffend die Auslagerung von Datenbearbeitungstätigkeiten bleiben im revidierten DSG praktisch unverändert. Neu können Personalverantwortliche oder andere Personen im Unternehmen aber mit einer Busse bis zu CHF 250'000 bestraft werden, wenn sie die Bestimmungen für die Auslagerung von Datenbearbeitungstätigkeiten vorsätzlich verletzen.

Wenn Personalabteilungen Datenbearbeitungstätigkeiten (bspw. die Lohnabrechnungen oder Buchhaltung) inner- oder ausserhalb des Konzerns auslagern, gilt dies in der Regel als Auslagerung von Datenbearbeitungstätigkeiten im Sinne des DSG. Das gleiche gilt, wenn für Evaluationen von Mitarbeitenden Programme von Drittanbietern verwendet werden.

Für solche Auslagerungen müssen so genannte. "Auftragsdatenbearbeitungsverträge" (ADV) mit den Auftragsdatenbearbeitern abgeschlossen werden. Ein solcher ADV muss neu eine Bestimmung für die vorgängige Genehmigung von Unterauftragsbearbeitern vorsehen. Ausserdem ist sicherzustellen, dass die Auftragsdatenbearbeiter angemessene Massnahmen zur Datensicherheit ergriffen haben. Zu diesem Zweck empfehlen wir entsprechende schriftliche Zusicherungen einzuholen und die Implementierung der Datensicherheitsmassnahmen vorab zu prüfen.

Schliesslich ist zu prüfen, ob gesetzliche oder vertragliche Geheimhaltungspflichten einer Auslagerung entgegenstehen könnten. Unserer Erfahrung nach ist dies bei Arbeitsverhältnissen selten der Fall. Läge ausnahmsweise eine solche Geheimhaltungspflicht vor (z.B. wegen einer vertraglichen Abmachung), wäre bspw. die Zustimmung der betroffenen Mitarbeitenden zur Auslagerung einzuholen.

HANDLUNGSEMPFEHLUNG

Wir empfehlen Arbeitgebern, Mitarbeitenden Vorlagen für die ADV direkt zur Verfügung zu stellen. Dabei ist es hilfreich, wenn diesen Vorlagen ein Merkblatt beigefügt ist, welches die Anwendung der Vertragspflichten und die Implementierung der Massnahmen erläutert.

AUSLANDDATENTRANSFER

Auch die Voraussetzungen für die Übermittlung von Daten ins Ausland bleiben im revidierten DSG grundsätzlich unverändert. Die vorsätzliche Verletzung der Bestimmungen kann jedoch auch hier neu eine persönliche Busse zur Folge haben.

Wenn Daten ins Ausland übermittelt werden, muss geprüft werden, ob die Empfänger der Daten in einem Land mit einem angemessenen Datenschutzniveau ansässig sind. Diese Länder sind in einer Liste im Anhang der DSV aufgeführt. Dazu gehören bspw. alle EU-Mitgliedstaaten und das Vereinigte Königreich. In diesen Fällen müssen grundsätzlich keine zusätzlichen Schutzmassnahmen für den Auslanddatentransfer ergriffen werden.

Werden Daten in ein Land übermittelt, das nicht auf dieser Liste aufgeführt ist (bspw. China oder Indien), müssen

Arbeitgeber ausreichende Schutzmassnahmen für eine solche Übermittlung implementieren. Hierzu gehören die Unterzeichnung der EU-Standardvertragsklauseln (SCC), die an das Schweizer Recht angepasst werden müssen, oder die interne Umsetzung verbindlicher Unternehmensregeln für konzerninterne Übermittlungen (BCR). BCR müssen vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) oder einer anderen zuständigen Aufsichtsbehörde vorgängig genehmigt werden, damit sie zum Einsatz kommen können.

HANDLUNGSEMPFEHLUNG

Wir empfehlen Arbeitgebern, ihre Mitarbeitenden über die genannten Bestimmungen aufzuklären und Vorlagen für die SCC vorzubereiten. Für Konzerne bietet es sich an, anstelle von BCRs (deren Genehmigungsprozess lange dauern kann) gruppeninterne Datenaustauschverträge (sog. Intra-Group Data Transfer Agreements) zu vereinbaren, welche die SCC beinhalten.

MELDUNG VON DATENSICHERHEITSVERLETZUNGEN

Gemäss dem revidierten DSG müssen Unternehmen den EDÖB oder betroffene Personen (bspw. Mitarbeitenden) so schnell wie möglich über eine Verletzung der Datensicherheit informieren. Die Verletzung dieser Pflicht untersteht keiner Busse.

Diese sofortige Meldepflicht greift allerdings nur, wenn die Verletzung ein hohes Risiko für die betroffenen Personen darstellt. Dies ist z.B. der Fall, wenn etwa ein hohes Risiko für Identitätsdiebstahl besteht oder besonders schützenswerte Daten (wie Gesundheitsdaten oder Strafregisterauszüge) gestohlen wurden. Ausserdem müssen die betroffenen Personen über solche Sicherheitsvorfälle informiert werden, wenn dies ihrem Schutz dient (bspw., wenn ein Risiko für Identitätsdiebstahl besteht oder sie ihre Kreditkarten sperren, ihre Bank informieren oder ihre Login-Daten ändern müssen). Eine Datensicherheitsverletzung kann vorliegen, wenn Mitarbeitende ihren Laptop oder andere mobile Geräte verlieren, E-Mails an falsche Adressaten schicken oder auf unsichere Links in E-Mails klicken. Abzuwägen ist jeweils, ob ein solcher Vorfall zu einem hohen Risiko für die betroffene Person führt oder nicht. Erst wenn ein objektiv hohes Risiko besteht, greift die sofortige Meldepflicht.

Die Meldungen an den EDÖB müssen während zwei Jahren nach dem Zeitpunkt der Meldung aufbewahrt werden. Auf der Website des EDÖB steht dafür ein Online-Meldeportal zur Verfügung.

HANDLUNGSEMPFEHLUNG

Unternehmen sollten innerhalb ihrer Organisation eine verantwortliche Stelle bezeichnen und die notwendigen Prozesse für die Meldepflichten implementieren.

Wir empfehlen den Arbeitgebern, für die interne Meldung durch betroffene Mitarbeitende Formulare vorzubereiten, mit denen die interne Meldung erfasst werden kann. Ausserdem empfehlen wir, die Mitarbeitenden regelmässig im Datenschutz bzw. insbesondere in Bezug auf die Datensicherheit zu schulen.

DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

Unternehmen müssen sogenannte Datenschutz-Folgenabschätzungen durchführen, wenn sie Datenbearbeitungsprozesse planen, die zu hohen Risiken für die betroffenen Personen führen können. Dies sind Risikoanalysen in Bezug auf eine bestimmte Datenbearbeitungstätigkeit sowie deren Auswirkungen auf die Persönlichkeit der betroffenen Personen.

Hohe Risiken bei Bearbeitungstätigkeiten liegen insbesondere vor, wenn umfangreich besonders schützenswerte Daten, wie Gesundheitsdaten oder Strafregisterauszüge, bearbeitet werden oder neue Technologien wie künstliche Intelligenz eingesetzt werden. Im Rahmen der Risikoanalyse sind Massnahmen zur Risikoreduktion zu identifizieren und zu implementieren. Kann das Risiko mit diesen Massnahmen nicht reduziert werden, muss der EDÖB konsultiert werden. Der EDÖB muss sodann innert drei Monaten seit Konsultation eine Handlungsempfehlung abgeben. Diese Risikoanalysen müssen dokumentiert und die Dokumentation muss für mindestens zwei Jahre nach der Datenbearbeitung aufbewahrt werden.

HANDLUNGSEMPFEHLUNG

Gerade im Rahmen der Mitarbeiterführung sowie in Bewerbungsprozessen setzen Arbeitgeber immer öfters neue Technologien und Programme ein, die zu hohen Risiken für betroffene Personen führen können (bspw.

Online-Bewerbungstools, welche gestützt auf künstlicher Intelligenz eine Vorauswahl der Stellenbewerbenden vornehmen). Wir empfehlen Arbeitgebern, Prozesse zu definieren, um die notwendigen Folgenabschätzungen aus datenschutzrechtlicher Sicht durchzuführen.

BEARBEITUNGSVERZEICHNIS

Unternehmen mit mehr als 250 Mitarbeitenden oder Unternehmen, die risikoreiche Datenbearbeitungstätigkeiten ausführen, haben neu ein Bearbeitungsverzeichnis zu führen. Damit sollen sämtliche Datenbearbeitungsprozesse des Unternehmens dokumentiert werden. Eine Verletzung dieser Pflicht untersteht keiner Busse.

Zwecks Nachvollziehbarkeit und Überprüfbarkeit muss das Verzeichnis gemäss revidiertem DSG u.a. Angaben betreffend Bearbeitungszweck, Kategorien der betroffenen Personen sowie Kategorien der bearbeiteten Personendaten, Übermittlungen von Daten ins Ausland, die Aufbewahrungsdauer und Massnahmen zur Gewährleistung der Datensicherheit enthalten.

Das Bearbeitungsverzeichnis dient als Ausgangspunkt für andere wesentlichen Pflichten gemäss revidiertem DSG; denn nur wer weiss, welche Daten zu welchem Zweck bearbeitet werden, kann auch die notwendigen Prozesse und Schutzmassnahmen implementieren und eine vollständige Datenschutzerklärung erstellen.

Während in der Regel die intern bezeichnete Datenschutzstelle oder der interne Datenschutzberater für die Führung des Bearbeitungsverzeichnisses verantwortlich ist, müssen diese durch die verschiedenen Abteilungen in ihrer Aufgabenerfüllung unterstützt werden. Entsprechend müssen auch Personalabteilungen für das Verzeichnis die Informationen liefern, die ihre Datenbearbeitungsprozesse betreffen, wie Bewerbungsprozess, Onboarding von Mitarbeitenden, Mitarbeiterführung oder Beendigung von Arbeitsverhältnissen.

HANDLUNGSEMPFEHLUNG

Wir empfehlen den Arbeitgebern, eine zuständige Person in der Personalabteilung zu ernennen, die für das Ausfüllen und die Aktualisierung des Bearbeitungsverzeichnisses im Rahmen des Arbeitsverhältnisses verantwortlich ist.

WEITERES

Neben den hier geschilderten Neuerungen wurden im revidierten DSG neu der Grundsatz "Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen" sowie das "Recht auf Datenherausgabe und -übermittlung" (sog. Recht auf Datenportabilität) eingeführt.

Die Straftatbestände werden im revidierten DSG erweitert und die maximalen Individualbussen wurden auf CHF 250'000 erhöht. Diese Straftatbestände greifen jedoch nur bei Vorsatz, wobei eventualvorsätzliches Handeln oder Unterlassen bereits ausreicht. Es handelt sich um Antragsdelikte, die nur bei entsprechenden Anträgen der geschädigten Personen von den Strafverfolgungsbehörden verfolgt werden. Wird eine Busse erteilt, erhält die verantwortliche Person einen Strafregistereintrag.

Weitere Informationen zum neuen Datenschutzrecht der Schweiz können in unseren allgemeinen Briefings zum revidierten DSG gefunden werden:

- Revised Swiss Data Protection Act: Not Ready Yet? Here's Your Guide
- The New Swiss Data Protection Law -Implementing Provisions Adopted
- Update: The Revised Federal Act on Data Protection – Get Ready Now
- The revised Data Protection Ac – A Quest for Adequacy

Autoren

Rehana Harasgama
Senior Associate
T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Rehana Harasgama ist Expertin im Daten-, Datenschutz- und Cybersicherheitsrecht. Sie berät Klienten bei komplexen Fragestellungen, wie z.B. bei grenzüberschreitenden Datenübermittlungen, der Umsetzung von Prozessen zur Meldung von Datensicherheitsverstössen, dem Outsourcing, Auskunftsbegehren und dem Umgang mit Mitarbeiterdaten.

Luljeta Morina
Associate
T: +41 58 261 50 58
luljeta.morina@baerkarrer.ch

Luljeta Morina berät schweizerische und ausländische Privatpersonen und Gesellschaften in den verschiedensten Gebieten des Schweizer Arbeitsrechts sowie in Fragen des allgemeinen Gesellschafts-, Handels-, und Vertragsrechts.