RECHTLICHES DATENMANAGEMENT IM KONZERN

Personendaten sind immer häufiger unverzichtbare Grundlage für die Wertschöpfungstätigkeit einer Unternehmung. Innerhalb eines Konzerns werden Personendaten zu verschiedenen Zwecken ausgetauscht, wobei Datenschutzanforderungen greifen. Rechtliches Datenmanagement setzt im Idealfall Standards für die gesamte Unternehmensgruppe bei der Bearbeitung von Personendaten. Dies ist in der Praxis oft schwierig umzusetzen. Eine betroffene Gruppengesellschaft sollte nicht auf einen allfälligen Gruppenentscheid warten, sondern auf Unternehmensstufe das rechtliche Datenmanagement aktiv vorantreiben.

Delia Fehr-Bosshard, LL.M., Anwältin

Datenschutzanforderungen nehmen zu

Vor allem die zunehmende Digitalisierung der Geschäftsprozesse und Leistungserbringung macht Daten zu einem immer wichtigeren Rohstoff für Unternehmen. Eine besondere Rolle nehmen dabei Personendaten ein, d.h. Informationen, die sich einer bestimmbaren Person zuordnen lassen. Jedes Unternehmen bearbeitet Personendaten regelmässig zumindest als Nebeneffekt (z.B. Daten der Arbeitnehmenden). In aller Regel ist die Beschaffung, Bearbeitung, Aufbewahrung und/oder Weitergabe dieser Personendaten Auslöser für die Anwendbarkeit von Datenschutzbestimmungen. Zunehmende rechtliche Anforderungen an Datenschutz und Datensicherheit – z.B. in der EU mit der Datenschutzgrundverordnung (DSGVO)[1] – erhöhen den Aufwand für Unternehmen.

In der Schweiz stehen wir (wieder) am Anfang der Totalrevision des Datenschutzgesetzes (DSG)[2]. Im Januar 2018 hat die Kommission für Wissenschaft, Bildung und Kultur des Nationalrates entschieden, die Revision zweizuteilen und die Totalrevision des DSG „ohne Zeitdruck“ anzugehen.[3] In der Schweiz ansässige Unternehmen und Gruppengesellschaften sind von der Revision in der EU aber auch betroffen. Dies gitl insbesondere bei der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der EU befinden, wenn die Datenverarbeitung im Zusammenhang steht mit einem Angebot von Waren oder Dienstleis-

---

1 Verordnung EU 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), verfügbar in Deutsch unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE.

2 Bundesgesetz über den Datenschutz, SR 235.1, verfügbar in Deutsch unter https://www.admin.ch/opc/de/classified-compilation/19920153/index.html.

3 Medienmitteilung der Kommission für Wissenschaft, Bildung und Kultur des Nationalrates vom 12. Januar 2018, verfügbar in Deutsch unter https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059.

tungen an diese Personen oder mit der Verhaltensbeobachtung dieser Personen in der EU.[4] Die DSGVO wird am 25. Mai 2018 wirksam.

Datenschutzerlasse wie die DSGVO und das Schweizer DSG, enthalten teils detaillierte Informationspflichten der Personendaten sammelnden und bearbeitenden Unternehmen, Auskunftsrechte der betroffenen Personen, Bearbeitungsgrundsätze, Anforderungen an die Rechtmässigkeit der Datenbearbeitung sowie Dokumentationspflichten. Unternehmen müssen unter Umständen Datenschutzfolgeabschätzungen schon im Vorfeld neuer Datenverwendungen durchführen, um die potentiellen Risiken für betroffene Personen abzuschätzen. Bei der Entwicklung von neuen Angeboten, Produkten und Leistungen müssen sie möglichst (technische) Vorkehrungen treffen und Voreinstellungen wählen, damit standardmässig nur ein Minimum an Daten überhaupt gesammelt wird (sog. "Privacy by design" und "Privacy by default").

Unter der DSGVO steigt das Sanktionsrisiko massiv: Neben Massnahmen wie der Anordnung konkreter Anpassungen von Bearbeitungspraktiken bis hin zum Verbot der Datenbeiarbeitung,[5] sieht die DSGVO insbesondere Bussen vor bis zum höheren Betrag von 4% des gesamten weltweit erzielten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr oder EUR 20'000'000.[6]

Rechtliches Datenmanagement ist unverzichtbar

Das optimale Management von Daten wird dadurch zu einem zentralen Erfolgsfaktor: Zum Datenmanagement gehören dabei alle Massnahmen, insbesondere konzeptioneller, technischer und organisatorischer Natur, mit denen der Einsatz der Ressource (Personen-)Daten gesteuert wird. Datenmanagement heisst aber nicht nur sicherzustellen, dass die benötigten und gewünschten Daten über Mitarbeitende und Kunden in hoher Qualität und Quantität zur Verfügung stehen, sondern beinhaltet auch die Pflege und den Schutz dieser Daten. Wer über Personendaten verfügt, hat nämlich nicht nur den Nutzen, sondern auch die Pflichten, z.B. in der EU-Terminologie als "Verantwortlicher" mit Entscheidungsgewalt über diese Personendaten.[7] Gutes rechtliches Datenmanagement ermöglicht die bestmögliche, effiziente Nutzbarmachung der Personendaten für die eigenen Geschäftsprozesse, unter Einhaltung der rechtlichen Anforderungen an Datenschutz und -Sicherheit.

(Rechtliches) Datenmanagement ist dabei bereits für eine mittelgrosse, eigenständige Gesellschaft eine Herausforderung: Eine Personalabteilung eines Schweizer KMU (z.B. mit Mitarbeitenden in Voll- und Teilzeit, mit Fest- und temporär Angestellten, Lernenden, langjährigen Mitarbeitenden und pensionierten ehemaligen Betriebsangehörigen) verfügt nur schon in ihren Personaldossiers über eine grosse Menge an Personendaten (z.B. Geburtsdaten der Mitarbeitenden und Familienmitgliedern, Adressen, Versicherungsleistungen, Saläre, Boni, Vorschüsse, Altersvorsorge, Krankheitsfälle, Arbeitszeugnisse, Beurteilungen, Beförderungen, etc.). Neben verschiedenen internen Nutzern (z.B. Personalverantwortliche, Ausbilder, IT-Verantwortliche, direkte Vorgesetzte) teilt die Arbeitgeberin diese Personendaten auch mit externen Dienstleistern (z.B. ausgelagerte Buchhaltungsanbieter, Revisoren) und unabhängigen Dritten (z.B. Ausgleichskassen, Pensionskassen, betriebliche Krankenversicherungen).

---

4 Art. 3 Abs. 2 DSGVO.
5 Art. 58 Abs. 2 DSGVO.
6 Art. 83 Abs. 5 DSGVO.
7 Vgl. die Definition in Art. 4 Ziff. 7 DSGVO.

Während der Umgang mit diesen Risiken bereits für die einzelne Gesellschaft herausfordernd ist, nimmt die Komplexität in einer Gruppenstruktur schlagartig zu. Jede einzelne Gruppengesellschaft ist dabei potentiell Beschafferin und Empfängerin von Personendaten (z.B. Arbeitgeberin, Lieferantin). Die einzelne Gesellschaft bearbeitet Personendaten in eigenem Interesse (z.B. Lohnbuchhaltung, Bestellabwicklung) und gibt diese für eigene Zwecke in- und ausserhalb der Gruppe weiter (z.B. Dienstleistungen einer zentralen Personalabteilung für die Gruppengesellschaft, zentrale Rechnungsstellung für Bestellungen). Die Gruppengesellschaften versorgen sich aber auch gegenseitig mit Personendaten ihrer Mitarbeitenden, Lieferanten und Kunden für die Zwecke der empfangenden Gruppengesellschaften oder im Interesse der Gruppe insgesamt (z.B. gruppenweites Karriereportal, Personalbeurteilung, Kundenvermittlung für Gruppengesellschaften, Kundenmanagementsysteme). Auch diese Weitergabe von Personendaten im Konzern, an Mutter-, Tochter- oder Schwestergesellschaften gilt als Weitergabe an Dritte und untersteht damit den datenschutzrechtlichen Anforderungen.

Die Datentransfers sind oft von einem vertraglichen Zweck gedeckt und dann auch unter der DSGVO an sich erlaubt. Bei einer Datenbekanntgabe an einen Dritten im Ausland kommen Anforderungen hinzu, wenn das Zielland kein sogenannt "adäquates" Schutzniveau bietet. Jeder dieser Datentransfers beinhaltet auch ein Risiko für die Datensicherheit des beauftragenden Unternehmens: Wenn der externe Anbieter der Lohnbuchhaltung seine eigenen IT Systeme lasch bewirtschaftet und unberechtigte Dritte Zugriff erhalten, schädigt dies nicht nur die betroffenen Mitarbeitenden, sondern unter Umständen auch die Arbeitgeberin, z.B. wenn Kontodaten für die Lohnzahlung offenbart werden. Auch Reputationsrisiken eines unsorgfältigen Behandelns von Daten nehmen zu, je grösser die Aufmerksamkeit der Öffentlichkeit für Themen wie Datensicherheit und Privatsphäre werden. Umso wichtiger ist das umfassende rechtliche Management der Datenbearbeitungspraxis im Unternehmen.

Entwicklung des rechtlichen Datenmanagements

Die einzelne Konzerngesellschaft oder die gesamte Gruppe kann mit einem einheitlichen Datenmanagement die Einhaltung der Sorgfaltspflichten besser gewährleisten. Eine einzelne Gruppengesellschaft kann dabei auch eine Vorbildfunktion innerhalb des Konzerns wahrnehmen und Datenschutz- und Sicherheit vorantreiben. Folgende Schritte, organisiert und durchgeführt mit in- und externer rechtlicher Unterstützung, eignen sich zur Festlegung der notwendigen Standards und Massnahmen zur Verbesserung des Datenmanagements:

- **Bestandesaufnahme, z.B. mit data mapping**: Data mapping schafft eine Auslegeordnung der bearbeiteten Personendaten und der existierenden Datenströme der gesamten Unternehmensgruppe. Ziel ist es, die bestehenden Bearbeitungsprozesse und Datenflüsse sowie ihre Grundlagen und die unternehmenseigenen Kontrollmechanismen zu identifizieren. Dazu gehört im Detail die Identifikation der Kategorien von betroffenen Personendaten (z.B. Adressdaten, Lohndaten, Gesundheitsdaten, Bestelldaten, Zahlungsverhalten etc.) und deren Bearbeitungszweck (z.B. Lohnabwicklung, Recruiting, zielgerichtete Werbung, Kreditentscheide). Darauf basierend erfolgt die Bestandsaufnahme zur Handhabung von Personendaten: z.B. welche Daten erhebt das Unternehmen, über wen, zu welchem Zweck, mit welcher Information an die betroffene Person, auf welcher Grundlage, mit welchen Standardverträgen, Vertragsklauseln etc.? Wem gibt das Unternehmen diese Daten weiter? Wie lange bewahrt es die Personendaten auf, wann löscht oder anonymisiert es die Daten standardmässig? Wichtig ist dabei auch die Identifikation, welche Personendaten (z.B. Lohndaten, Bestellverhalten) und in welchen Bereichen (z.B. Personal, Marketing)

diese für das Tagesgeschäft unverzichtbar sind. Weiter sollen die betroffenen Daten unterteilt werden nach Sensitivität: Gesundheitsdaten der Mitarbeitenden sind z.B. heikler als öffentlich verfügbare Adressdaten. Zur Informationssammlung eignen sich Unterlagen über bestehende Standards, Datenschutzbestimmungen, Verträge, etc. aber auch Interviews und Workshops. Data mapping wird schnell sehr aufwändig. Falls eine Konzernleitung diesen Aufwand nicht zu tragen bereit ist, empfiehlt es sich trotzdem auch für eine einzelne Gruppengesellschaft, die ein- und ausgehenden Ströme von Personendaten aus Sicht der einzelnen Unternehmung zu erfassen.

- **Identifikation des Handlungsbedarfs mittels gap analysis:** Die gelebten Verhältnisse müssen auf ihre Übereinstimmung mit den rechtlichen Anforderungen an die Information, Einwilligung, Grundlage für die Datenbearbeitung, Datensicherheit etc. geprüft werden. Daraus ergeben sich die zu schliessenden Lücken, die für das Unternehmen ein Risiko darstellen. Diese sind in einem risikobasierten Ansatz weiter nach dem Reputations- und Sanktionsrisiko und nach der Dringlichkeit zu kategorisieren: Welche Praktiken der Gruppengesellschaft sind nicht konform mit der DSGVO bzw. dem anwendbaren Datenschutzgesetz (wie das DSG) und aus welchen Gründen? Auf welche Grundlage stützt sich das Unternehmen bei der Bearbeitung von Personendaten? Für welche Datenbearbeitung und –Weitergabe fehlt die ausreichende Grundlage? Wo liegen dabei die grössten Risiken? Wenn der Konzernleitungsentscheid fehlt, sind die Lücken aus Sicht des einzelnen Unternehmens zu bestimmen.
- **Massnahmen:** Gestützt auf die festgestellten Defizite und Risiken kann die einzelne Gruppengesellschaft Handlungsbedarf ableiten, um die identifizierten Lücken risikoadäquat zu schliessen. Zu ergreifende Änderungen umfassen vor allem technische Regeln (v.a. im Bereich IT, z.B. technische Zugangsbeschränkungen, Zwei-Faktor-Authentifizierung, standardmässige Pseudonymisierung oder Anonymisierung etc.) und organisatorische Anpassungen (z.B. Festlegung von Standardverfahren und –Dokumenten zur Information und Einwilligung, Definition von Zuständigkeiten für Auskunftsgesuche etc.). Zur Festlegung der zu ergreifenden technischen und organisatorischen Massnahmen sind in dieser Phase auch der zeitliche Ablauf der Implementierung und allfällige Budgetrestriktionen detailliert zu klären. Auf dieser Stufe besteht erneut eine Gelegenheit, weitere Gruppengesellschaften oder sogar die Konzernleitung mit ins Boot zu holen, um einen gruppenweiten Massnahmeplan auszuarbeiten. Auf Ebene jeder involvierten Gesellschaft muss die Unternehmensleitung die Massnahmen genehmigen.
- **Implementierung:** Im Hinblick auf das Wirksamwerden der DSGVO im Mai 2018 sind viele Unternehmen schon in der Implementierungsphase. Auch wenn der Idealfall eine gruppenweit einheitliche Inkraftsetzung der Massnahmen umfasst, ist dies aus unserer Erfahrung in der Praxis oft illusorisch. Um die eigenen Sorgfaltspflichten als Unternehmen wahrzunehmen, ist eine gestufte Implementierung der dringlichsten Massnahmen auf Ebene der lokalen Gruppengesellschaft dem Abwarten eines globalen Konzernentscheids unter Umständen vorzuziehen. Die Implementierung umfasst auch operationelle Änderung. Regelmässig im Vordergrund stehen aber die Schulung und Instruktion der Mitarbeitenden.

"Data Awareness" ist für Datenmanagement zentral

Bei der Implementierung von Massnahmen kommt dem Faktor "Mensch" eine zentrale Rolle zu: Der eidgenössische Datenschutzbeauftragte (EDÖB) empfiehlt eine "eingehende Information und Sensibilisierung der Mitarbeiter in Verbindung mit technisch-organisatorischen Präventionsmassnahmen"[8], um eine fahrlässige Datenschutzverletzung zu vermeiden. Was auf den ersten Blick als sehr pauschale Aussage erscheint, trifft den Kern der Sorgfaltspflichten eines Unternehmens im Bereich Datenschutz: Technische und organisatorische Massnahmen sind unerlässlich, um einen adäquaten Schutz von Personendaten auf Unternehmensstufe zu gewährleisten. Der Faktor "Mensch" ist und bleibt der eigentliche "Wackelkandidat". Im Bereich der Datensicherheit zeigt sich, dass regelmässig menschliches Versagen, Unachtsamkeit oder Unwissen eigentliche Ursachen für Datenlecks sind. Die Unternehmung kann ihren Sorgfaltspflichten nur effektiv nachkommen, wenn sie mit Information, Aufklärung, Training und verbindlichen Weisungen das Bewusstsein jedes einzelnen Mitarbeitenden für die Bedeutung von Personendaten und deren Sicherheit schärft. Mitarbeitende (von der Aushilfe bis zur Führungsspitze) sind primäre Zielpersonen dieser Massnahmen. "Data Awareness" verlangt aber auch in der Kommunikation mit anderen Gruppengesellschaften einheitliche Standards. Eine Gruppengesellschaft kann dabei ihre Leitlinien für die gruppeninterne und –externe Weitergabe von Personendaten in aller Regel besser durchsetzen und rechtfertigen, wenn sie intern auf dem Niveau der eigenen Gesellschaft sorgfältiges Datenmanagement betreibt und Datenschutz nicht nur auf dem Papier festhält, sondern aktiv lebt. Je konsequenter und verlässlicher das rechtliche Datenmanagement auf Stufe der einzelnen Unternehmung ist, desto eher folgen andere Gruppengesellschaften dem guten Vorbild. Gruppenweit gelebte Standards vereinfachen wiederum die Einhaltung der Datenschutzanforderungen und wirken sich als Nebeneffekt gut auf die Reputation des gesamten Konzerns aus.

VISCHER AG
www.vischer.com
Schützengasse 1 8021 Zürich Schweiz Tel +41 58 211 34 00
Aeschenvorstadt 4 4010 Basel Schweiz Tel +41 58 211 33 00

8 EDÖB, Verantwortlichkeit, verfügbar in Deutsch unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/verantwortlichkeit.html (zuletzt besucht am 28. Februar 2018).