Mitarbeitendendatenschutz – der oft vergessene Teil des Compliance Frameworks?

Viele Unternehmen haben sich bei ihren Datenschutz-Compliance-Projekten in einer ersten Phase nicht oder nicht spezifisch mit dem Mitarbeitendendatenschutz befasst. Wenn überhaupt, war die Bearbeitung von Personendaten über Mitarbeitende Thema bei der Erstellung des Verzeichnisses über die Datenbearbeitungen. Dies ergibt bei einem schrittweisen Vorgehen Sinn.

Von Michael Reinle

Zahlreiche «allgemeine» Compliance-Massnahmen wie z. B. Prozesse für Auskunftsgesuche, Datenschutz-Folgenabschätzungen oder Verletzungen der Datensicherheit sind auch im Bereich Mitarbeitendendatenschutz relevant. Dasselbe gilt für die erstellten Auftragsbearbeitungstemplates. Die nachrangige Berücksichtigung des Mitarbeitendendatenschutzes ist auch deshalb «verzeihlich», weil die Personalabteilungen erfahrungsgemäss über eine sehr hohe Sensibilisierung für Datenschutzfragen verfügen. Gleichwohl bringt das neue Datenschutzgesetz («DSG») Pflichten mit sich, welche beim Mitarbeitendendatenschutz zur Implementierung neuer Massnahmen führen. Mitarbeitendendatenschutz darf nicht vergessen werden. Vielmehr ist der Mitarbeitendendatenschutz in das bestehende Datenschutz-Compliance-Framework zu integrieren.

Welche Massnahmen stehen im Vordergrund?

Umsetzung der Informationspflicht

Art. 19 ff. DSG verankern neue, formelle Informationspflichten. Unter dem alten DSG bestand «lediglich» eine Transparenzpflicht. Die Transparenz konnte ohne formelle Information erfüllt werden. Transparenz über Datenbeschaffungen und -bearbeitungen konnte auch aus dem Kontext erstellt werden. Neu muss über jede Datenbeschaffung und -bearbeitung informiert werden, es sei denn, es bestünde eine Ausnahme von der Informationspflicht (Art. 20 DSG). Die Informationspflicht gilt auch dann – insbesondere dann –, wenn die Personendaten nicht direkt bei der betroffenen Person beschafft werden, z. B. wenn Informationen über Mitarbeitende bei Drittpersonen eingeholt werden.

Art. 19 DSG enthält einen Mindestkatalog an Informationen, welche den betroffenen Personen übermittelt werden müssen (z. B. Bearbeitungszweck, Empfänger oder Kategorien der Empfänger von Personendaten etc.). Informationen über diesen Mindestkatalog hinaus sind lediglich in besonderen Konstellationen erforderlich.

Umstritten ist, ob die Informationspflicht nach Art. 19 DSG auf die Bearbeitung von Mitarbeitendendaten anwendbar ist. Eine Information kann nach Art. 20 Abs. 1 lit. b DSG unterbleiben, wenn die betreffende Datenbearbeitung gesetzlich vorgesehen ist. Mitunter wird Art. 328b OR als gesetzliche Grundlage erwähnt. Auch wenn es im arbeitsrechtlichen Bereich sehr viele gesetzliche Pflichten zur Datenbearbeitung gibt (z. B. im Zusammenhang mit den Sozialversicherungen), kann Art. 328b OR nicht als gesetzliche Grundlage im Sinne von Art. 20 Abs. 1 lit. b DSG gelten. Art. 328b OR stellt vielmehr eine Lex specialis zu den Datenbearbeitungsgrundsätzen im DSG dar (Zweckbindungsgebote und Grundsatz der Verhältnismässigkeit). Art. 328b OR sagt nicht, dass und wann Personendaten über Mitarbeitende zu bearbeiten sind. Art. 328b OR gibt lediglich materielle Grundsätze vor, falls Mitarbeitendendaten bearbeitet werden. Auch sonst ist jeweils genau zu prüfen, ob eine gesetzliche Bestimmung die Bearbeitung von Personendaten erforderlich macht.

Im Ergebnis ist Art. 19 DSG auf die Bearbeitung von Mitarbeitendendaten anwendbar, auch wenn gewisse Datenbearbeitungen unter die Ausnahme von Art. 20 Abs. 1 lit. b DSG fallen können und in der Information nicht mitenthalten sein müssen.

Zur Umsetzung der Informationspflicht können die Unternehmen eine Datenschutzerklärung erstellen, wie dies auch für andere Datenbearbeitungen getan wird. Die Unternehmen können sich betreffend Struktur und Aufbau der Datenschutzerklärung an ihren anderen Datenschutzerklärungen orientieren.

Empfehlenswert ist es, die Datenschutzerklärung als separates Dokument auszugestalten. Die Datenschutzinformation sollte nicht in den Arbeitsvertrag inkorporiert oder zum Bestandteil des Arbeitsvertrags erklärt werden. Bei der Erfüllung der Informationspflicht handelt es sich um eine blosse Information bzw. Informationserklärung. Es handelt sich

nicht um einen Vertrag, welcher von den Mitarbeitenden angenommen werden muss. Die Ausgestaltung als blosse Informationserklärung erleichtert zukünftige Anpassungen. Zukünftige Anpassungen treten ohne Zustimmung der Mitarbeitenden in Kraft. Möchte man aus Beweisgründen eine schriftliche Erklärung der Mitarbeitenden einholen, ist die Formulierung entscheidend. Okay ist: «Ich erkläre hiermit, dass ich die Datenschutzerklärung zur Kenntnis genommen habe.» Nicht okay ist: «Ich stimme hiermit der Datenschutzerklärung zu.»

Erfahrungsgemäss ist es sinnvoll, für gewisse Datenbearbeitungen zusätzlich zur allgemeinen Mitarbeitendendatenschutzerklärung separate Informationen zu erstellen. Dies ergibt z. B. bei Überwachungsmassnahmen Sinn, bei denen in Überwachungsreglementen nebst anderen Themen auch die damit zusammenhängenden Datenbearbeitungen besprochen werden. Dasselbe gilt für freiwillig eingerichtete Whistleblowing-Hotlines. Sinnvoll sind separate Datenschutzinformationen auch dann, wenn die Personalabteilung neue HR-Tools testen möchte oder wenn beim Einsatz von HR-Tools der Anbieter des Tools für gewisse Datenbearbeitungen als Verantwortlicher oder gemeinsamer Verantwortlicher mit dem Arbeitgeber agiert. Es gibt z. B. Tools, bei denen der Arbeitgeber in einem ersten Schritt dem Anbieter des Tools die Namen und E-Mail-Adressen von Mitarbeitenden weitergibt, um Konten zu erstellen. Nachher werden die Mitarbeitenden über die Kontenerstellung informiert und müssen sich sodann im Tool anmelden. Für die weiteren Datenbearbeitungen ist der Anbieter des Tools der Verantwortliche. Ergebnisse der Datenbearbeitungen im Tool werden dem Arbeitgeber weitergegeben, bzw. dieser erhält Zugriff auf diese Ergebnisse. Der Arbeitgeber wertet sodann diese Ergebnisse aus und bearbeitet diese als selbstständiger Verantwortlicher weiter. In dieser Konstellation ist ein blosser Verweis auf die Datenschutzerklärung des Tool-Anbieters nicht ausreichend. Der Arbeitgeber muss über die Datenbearbeitungen, für welche er selbst Verantwortlicher ist, eigenständig informieren.

- Die Bearbeitung von Mitarbeitendendaten fällt unter die Informationspflicht nach Art. 19 DSG. Eine Information ist somit zwingend erforderlich, ausser eine spezifische Datenbearbeitung sei gesetzlich vorgesehen.
- Es genügt grundsätzlich die Einhaltung des Mindestkatalogs an Informationen nach Art. 19 DSG. Bei der Information über Empfänger von Mitarbeitendendaten genügt es, wenn die Kategorien der Empfänger angegeben werden. Dies kann aus Gründen des Geschäftsgeheimnisses sinnvoll sein, oder weil gewisse Drittdienstleister regelmässig gewechselt werden.
- Die Information sollte in einer separaten Erklärung erfolgen. Die Information sollte nicht in den Arbeitsvertrag integriert oder zu dessen Bestandteil erklärt werden.
- Es kann sinnvoll sein, für gewisse Datenbearbeitungen eine eigene Datenschutzinformation zu erstellen (z. B. bei Softwarelösungen, bei denen der Anbieter der Softwarelösung für gewisse Datenbearbeitungen eigener Verantwortlicher oder gemeinsamer Verantwortlicher ist).

Verzeichnis der Bearbeitungstätigkeiten

Falls die Bearbeitung von Mitarbeitendendaten noch nicht ins allgemeine Verzeichnis der Bearbeitungstätigkeiten integriert wurde, sollte dies nachgeholt werden – sofern überhaupt ein Verzeichnis zu erstellen ist.

Es ist hierbei entscheidend, dass der interne Verantwortliche für Datenschutzfragen eng mit der Personalabteilung zusammenarbeitet.

Bei der Erstellung des Verzeichnisses dürfen verschiedene Datenbearbeitungen zusammengefasst werden, wenn diese vergleichbar sind und z. B. demselben Zweck dienen. Allerdings sollten auch nicht zu viele Datenbearbeitungen zusammengefasst werden. Ein einziger Eintrag als «Lohnadministration» ist nicht zu empfehlen. Die Lohnadministration im weiteren Sinne setzt sich aus zahlreichen Datenbearbeitungen zusammen, welche nicht alle vergleichbar sind oder einen Konnex haben.

Ansonsten gibt es im Vergleich zum «normalen» Verzeichnis der Bearbeitungstätigkeiten keine Besonderheiten.

- Die Bearbeitungen von Mitarbeitendendaten sind im Verzeichnis der Bearbeitungstätigkeiten zu ergänzen.
- Bei der Ergänzung ist eine enge Zusammenarbeit zwischen dem Verantwortlichen für Datenschutzfragen und der Personalabteilung entscheidend.

Datenschutz-Folgenabschätzung

Nach Art. 22 DSG muss der Verantwortliche vorgängig eine Datenschutz-Folgenabschätzung erstellen, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.

Nach Art. 22 Abs. 2 DSG kann namentlich ein hohes Risiko vorliegen, wenn besonders schützenswerte Personendaten in hohem Umfang bearbeitet werden. Im Personalbereich werden regelmässig besonders schützenswerte Personendaten bearbeitet. Nicht jede Bearbeitung von Mitarbeitendendaten stellt jedoch ein hohes Risiko dar. Es ist im Einzelfall zu entscheiden, ob ein hohes Risiko gegeben ist.

Besonders wichtig bei Mitarbeitendendaten ist Art. 22 Abs. 4 DSG. Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind. Es ist jedoch wiederum sorgfältig zu prüfen, ob eine gesetzliche Bestim-

mung effektiv zur Datenbearbeitung verpflichtet.

Zur Umsetzung der Pflichten im Zusammenhang mit der Datenschutz-Folgenabschätzung ist es besonders wichtig, dass die Personen, welche über die Durchführung einer Datenschutz-Folgenabschätzung befinden müssen, frühzeitig über neue Datenbearbeitungen oder Änderungen bestehender Datenbearbeitungen informiert werden. Im Gegensatz zu Datenbearbeitungen ausserhalb des Personalbereichs, wo es zahlreiche unterschiedliche Data Owners oder Project Owners geben kann, sollte diese frühzeitige Erkennung im Personalbereich weniger schwierig sein. Es ist wichtig, dass sich die Personalabteilung auch frühzeitig genug an den internen Verantwortlichen für Datenschutzfragen wendet.

Die Unternehmen sollten auch für Datenschutz-Folgenabschätzungen im Bereich der Mitarbeitendendaten interne Weisungen oder Guidelines erstellen. Dabei kann primär auf bestehende Weisungen für andere Datenbearbeitungen abgestellt werden. Besonderheiten können sich jedoch bei der Datenschutz-Folgenabschätzung im Bereich Mitarbeitendendaten hinsichtlich der Verantwortlichkeiten ergeben (z. B. dass die Personalabteilung selbst für die Durchführung der Datenschutz-Folgenabschätzung zuständig ist).

Zudem sollten bei den Checklisten – «Wann ist eine DSFA erforderlich» – spezifische Beispiele aus dem Arbeitsbereich eingebaut werden. Letztlich sollen diese Checklisten der Personalabteilung dabei helfen, hohe Risiken zu erkennen. Man kann sich dabei an den Guidelines der EU-Behörden oder der nationalen Datenschutzbehörden in EU-Mitgliedstaaten bzw. von UK orientieren. Diese enthalten zwar nur wenige Beispiele, welche spezifisch mit Mitarbeitendendaten zu tun haben, doch lassen sich gewisse Beispiele auf den Arbeitsbereich umwandeln.

- Bei der Bearbeitung von Mitarbeitendendaten können sich hohe Risiken ergeben, da regelmässig besonders schützenswerte Personendaten bearbeitet werden. Immer mehr werden solche Daten analysiert und ausgewertet und erzielen nachher eine rechtliche Wirkung (z. B. eine Beförderung). Im Arbeitsbereich werden auch vermehrt neue Technologien eingesetzt – nicht nur für die Überwachung –, welche in hohem Umfang Mitarbeitendendaten automatisiert bearbeiten. Konstellationen, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist, werden zukünftig zunehmen.
- Die Personalabteilung sollte den internen Verantwortlichen für Datenschutzfragen möglichst frühzeitig über neue Datenbearbeitungen oder die Änderung bestehender Datenbearbeitungen informieren.
- Die Unternehmen sollten Guidelines für die Durchführung von Datenschutz-Folgenabschätzungen im Personalbereich erstellen. Diese können sich primär an bestehenden Guidelines für andere Datenbearbeitungen orientieren. Besonderheiten sind allerdings zu berücksichtigen (Verantwortlichkeiten der Personalabteilung, spezifische Beispiele von hohen Risiken im Personalbereich).

Betroffenenrechte

Die Mitarbeitenden verfügen über dieselben Betroffenenrechte wie andere betroffene Personen. Zu nennen sind das Auskunftsrecht, das Löschungsrecht, das Recht auf Datenportabilität, das Widerspruchsrecht etc. Die rechtlichen Rahmenbedingungen bei der Ausübung dieser Rechte unterscheidet sich ebenfalls nicht im Vergleich zu anderen betroffenen Personen.

Gleichwohl kann sich die Implementierung spezifischer Prozesse für die Geltendmachung der Betroffenenrechte durch Mitarbeitende empfehlen. Es ist z. B. empfehlenswert, wenn sich die Mitarbeitenden für die Geltendmachung ihrer Betroffenenrechte an die Personalabteilung wenden müssen und nicht an die allgemeine E-Mail-Adresse wie andere betroffene Personen. Hierüber sind die Mitarbeitenden zu informieren. Es ist des Weiteren sinnvoll, wenn die Personalabteilung und nicht der interne Verantwortliche für Datenschutzfragen für die Beantwortung der Gesuche hauptverantwortlich ist. Der Verantwortliche für Datenschutzfragen sollte jedoch beratend zur Verfügung stehen und die Antwort auf die Gesuche vor deren Versand anschauen.

Die Verantwortlichkeit der Personalabteilung ist sinnvoll und wichtig, weil Auskunftsgesuche durch Mitarbeitende regelmässig mit arbeitsrechtlichen Fragen im Zusammenhang stehen (z. B. bei Auskunftsgesuchen in zeitlichem Zusammenhang mit einer arbeitsrechtlichen Streitigkeit). In diesen Konstellationen ist es wichtig, dass die Beantwortung des datenschutzrechtlichen Auskunftsgesuchs mit dem Vorgehen bei der arbeitsrechtlichen Frage koordiniert wird.

In solchen Konstellationen ist jeweils insbesondere auch zu prüfen, ob eine Ausnahme vom Auskunftsgesuch besteht, z. B. ein rechtsmissbräuchliches Auskunftsgesuch oder überwiegende Interessen Dritter (z. B. anderer Mitarbeitender). Zu beachten ist in diesem Zusammenhang, dass die Verweigerung einer Auskunft (z. B. gestützt auf Rechtsmissbrauch) nach Art. 60 DSG nicht strafrechtlich sanktioniert ist. Strafrechtlich sanktioniert ist nur die falsche oder unvollständige Auskunft.

- Die Geltendmachung der Betroffenenrechte durch Mitarbeitende untersteht denselben gesetzlichen Anforderungen wie die Geltendmachung durch andere betroffene Personen.

- Gleichwohl kann die Implementierung separater Prozesse für die Geltendmachung der Betroffenenrechte durch Mitarbeitende sinnvoll sein. Es kann z.B. sinnvoll sein, dass sich die Mitarbeitenden betreffend Betroffenenrechte zunächst an die Personalabteilung wenden müssen. Die Personalabteilung sollte auf jeden Fall in den Prozess involviert sein, da Auskunftsgesuche von Mitarbeitenden regelmässig in einem Konnex mit arbeitsrechtlichen Fragen stehen (z.B. einer arbeitsrechtlichen Streitigkeit). Die Beantwortung von Auskunftsgesuchen ist mit diesen arbeitsrechtlichen Fragen zu koordinieren.

Auftragsbearbeitung und Datentransfers ins Ausland

Die gesetzlichen Anforderungen für die Auftragsbearbeitung und Datentransfers ins Ausland sind bei Mitarbeitendendaten gleich wie bei anderen Personendaten. Es können daher die bereits bestehenden Templates für Auftragsbearbeitungsverträge und Datentransfers verwendet werden.

Wichtig ist, dass Auftragsbearbeitungen und Datentransfers im Personalbereich nicht vergessen gehen. Es ist wichtig, auch im Personalbereich eine Übersicht über Drittdienstleister bzw. Datenempfänger im Ausland zu erstellen. Sodann ist anhand dieser Übersicht zu prüfen, bei welchen Drittdienstleistern Auftragsbearbeitungsverträge oder spezifische Massnahmen für Datentransfers ins Ausland erforderlich sind. In einem letzten Schritt sind sodann die Massnahmen (Abschluss von Auftragsbearbeitungsverträgen oder Datentransferverträgen) zu implementieren.

Wichtig ist wiederum die enge Zusammenarbeit zwischen der Personalabteilung und dem internen Verantwortlichen für Datenschutzfragen. Die Personalabteilung sollte jeweils den internen Verantwortlichen für Datenschutzfragen auch darüber informieren, wenn neue Drittdienstleister oder Datenempfänger im Ausland hinzukommen.

- Falls noch nicht erfolgt, sollte die Personalabteilung zusammen mit dem internen Verantwortlichen für Datenschutzfragen eine Übersicht über alle Drittdienstleister und Datenempfänger im Ausland für den Personalbereich erstellen. Nachher ist zu prüfen, ob mit diesen Drittpersonen entsprechende Verträge abzuschliessen sind (Auftragsbearbeitungsverträge oder Datentransferverträge).
- Entscheidend ist eine gute Koordination zwischen der Personalabteilung und dem internen Verantwortlichen für Datenschutzfragen.

Verletzung der Datensicherheit

Betreffend Massnahmen bei Verletzung der Datensicherheit gibt es bei Mitarbeitendendaten im Vergleich zu anderen Personendaten keine Unterschiede. Es drängen sich hierbei auch keine abweichenden Prozesse auf.

Wichtig ist, dass die Mitarbeitenden der Personalabteilung speziell betreffend Massnahmen zur Verhinderung der Verletzung der Datensicherheit sowie auch betreffend das Vorgehen bei einer Verletzung der Datensicherheit geschult werden. Die Verletzung der Datensicherheit im Bereich der Mitarbeitendendaten kann zu einem substanziellen Schaden führen, da es sich regelmässig um besonders schützenswerte Daten handelt.

Wichtig ist zudem, dass die Massnahmen zur Gewährleistung der Datensicherheit auch auf den Personalbereich erstreckt werden. Auch für den Personalbereich sind spezifische technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit zu konzipieren und zu implementieren, falls dies noch nicht geschehen ist.

- Betreffend die Massnahmen bei Verletzung der Datensicherheit sind für die Mitarbeitendendaten keine gesonderten Prozesse erforderlich. Die Mitarbeitenden im Personalbereich sollten jedoch speziell geschult werden.
- Besonders wichtig ist die Prävention von Verletzungen der Datensicherheit. Falls noch nicht erfolgt, sind spezifische technische und organisatorische Datensicherheitsmassnahmen für den Personalbereich zu konzipieren und zu implementieren.

Aufbewahrungsdauer

Für die Aufbewahrung von Mitarbeitendendaten bzw. von Datenträgern mit Mitarbeitendendaten sind spezifische Aufbewahrungsregelungen festzulegen. Es besteht grundsätzlich ein überwiegendes Interesse daran, diese Unterlagen bis zum Ablauf der gesetzlichen Verjährungsfristen für arbeitsrechtliche Ansprüche aufzubewahren. Viele Unterlagen können daher bis zu zehn Jahre nach Beendigung des betreffenden Arbeitsverhältnisses aufbewahrt werden. Eine kürzere Aufbewahrungsfrist gilt bei den Bewerbungsunterlagen von abgewiesenen Bewerbenden, sofern diese nicht einer längeren Aufbewahrung zugestimmt haben. Die konkreten Aufbewahrungsdauern sind im Einzelfall festzulegen.

Falls vorhanden, können die Aufbewahrungsfristen für Mitarbeitendendaten in einen allgemeinen Record Retention Schedule des Unternehmens eingebaut werden. Ansonsten sollte ein separates Dokument erstellt werden, in welchem die Aufbewahrungsfristen für die relevantesten Unterlagen im Personalbereich festgelegt werden. Das Dokument sollte auch Verantwortlichkeiten betreffend die Prüfung einer Verlängerung der Aufbewahrungsdauer oder die Prüfung der Löschung der Unterlagen festlegen.

- Die zulässige Aufbewahrungsdauer von Mitarbeitendendaten richtet sich primär nach den gesetzlichen Verjährungsfristen für arbeitsrechtliche Ansprüche. Die konkreten Aufbewahrungsdauern sind im Einzelfall festzulegen.

- Die Aufbewahrungsdauer für Mitarbeitendendaten sollte entweder in einen bestehenden «Record Retention Schedule» integriert werden, oder das Unternehmen sollte ein separates Dokument erstellen, in welchem die Aufbewahrungsdauer und Verantwortlichkeiten im Zusammenhang mit Mitarbeitendendaten festgelegt werden.

Weitere Massnahmen?

In Aufsätzen zum Mitarbeitendendatenschutz werden jeweils weitere Massnahmen erwähnt, z. B. Massnahmen im Bereich der Mitarbeitendenüberwachung, bei internen Untersuchungen, bei Video- und Fotoaufnahmen etc.

Es ist sicherlich wichtig zu erwähnen, dass bei den oben genannten Konstellationen Datenschutz eine relevante Bedeutung erhält und somit zu berücksichtigen ist. Allerdings ist in den genannten Konstellationen – nebst der neuen Informationspflicht und der allfälligen Durchführung einer Datenschutz-Folgenabschätzung – vor allem die Einhaltung der Datenbearbeitungsgrundsätze (Treu und Glauben, Transparenzgrundsatz, Zweckbindungsgrundsatz, Richtigkeitsgrundsatz, Verhältnismässigkeitsprinzip) besonders relevant. Bei den Datenbearbeitungsgrundsätzen gibt es im Vergleich zum alten DSG inhaltlich keine massgebenden Änderungen. Datenbearbeitungen, welche unter dem alten DSG die Bearbeitungsgrundsätze eingehalten haben, tun dies auch nach revidiertem DSG. Von daher sind diesbezüglich allein wegen der Revision des DSG keine neuen Massnahmen erforderlich. Entscheidend ist vielmehr, dass – was unter dem alten DSG nicht immer korrekt gemacht wurde – die Datenbearbeitungsgrundsätze bei all diesen Konstellationen berücksichtigt und umgesetzt werden.

Zuletzt: Schulung

Ein wichtiger Bestandteil des Compliance Frameworks ist die Schulung derjenigen Mitarbeitenden, welche Personendaten bearbeiten.

Dies gilt auch – bzw. wegen der häufig besonders schützenswerten Natur der Mitarbeitendendaten vor allem – bei Mitarbeitendendaten. Es ist wichtig, dass die Mitarbeitenden der Personalabteilung über den korrekten Umgang mit Mitarbeitendendaten regelmässig geschult werden.

Es ist hierbei empfehlenswert, separate Schulungen für die Mitarbeitenden der Personalabteilung durchzuführen. Dies erlaubt es, die gesetzlichen Rahmenbedingungen mithilfe konkreter Beispiele aus dem Personalbereich darzustellen.

- Wesentlicher Bestandteil des Compliance Frameworks ist die regelmässige Schulung über den korrekten Umgang mit Mitarbeitendendaten.
- Die Schulung sollte separat für die Mitarbeitenden der Personalabteilung durchgeführt werden, damit die gesetzlichen Rahmenbedingungen mit konkreten Beispielen aus dem Personalbereich erläutert werden können.

Exkurs: Pensionskassen

Bei vielen Unternehmen ist die Personalabteilung auch für sozialversicherungsrechtliche Themen zuständig und hält z. B. auch den Kontakt zu den Pensionskassen-Stiftungen. Gewisse Unternehmen haben eigene Pensionskassen-Stiftungen gegründet.

Es wird daher regelmässig die Frage gestellt, ob man die Datenbearbeitungen der Pensionskassen-Stiftungen gleich zusammen mit dem Mitarbeitendendatenschutz erfassen kann. Dies bietet sich jedoch nicht an.

Erstens handelt es sich bei den Pensionskassen-Stiftungen um eigenständige Rechtspersönlichkeiten und damit um eigenständige datenschutzrechtlich Verantwortliche – sie haben je nach Datenbearbeitung eine gemeinsame Verantwortung mit den Servicegesellschaften, welche für den operativen Betrieb der Pensionskasse zuständig sind. Die Pensionskassen-Stiftungen sind somit selbst für die Compliance mit dem DSG verantwortlich – was nicht zwingend bedeutet, dass die Umsetzung von Compliance-Massnahmen nicht delegiert werden könnte. Zweitens – und umso wichtiger – die Pensionskassen-Stiftungen qualifizieren im obligatorischen Teil als Bundesorgane und müssen daher für die Datenbearbeitungen im obligatorischen Teil die Bestimmungen des DSG einhalten, welche sich an die Bundesorgane richten. Gemäss DSG und auch der dazugehörigen Datenschutzverordnung gibt es gewisse Compliance-Massnahmen, welche von Bundesorganen – im Gegensatz zu privaten Verantwortlichen – zwingend umzusetzen sind. So müssen Pensionskassen-Stiftungen praktisch immer ein Bearbeitungsreglement erstellen (Art. 6 DSV). Strengere Vorgaben bestehen für Bundesorgane auch bei der Protokollierung (Art. 4 DSV). Zudem müssen Bundesorgane zwingend einen Datenschutzberater ernennen (Art. 10 DSG). Auch bei anderen Pflichten gemäss DSG gibt es gewisse Abweichungen bei Bundesorganen.

Es empfiehlt sich daher, bei Pensionskassen-Stiftungen ein separates Compliance-Projekt durchzuführen. Gewisse Massnahmen und Dokumente, z. B. interne Guidelines und Prozesse, können zwar als Ausgangspunkt auch bei den Pensionskassen-Stiftungen angewandt werden, doch ist jeweils zu prüfen, ob die Dokumente auch die spezifischen Pflichten für Bundesorgane einhalten. Gegebenenfalls sind die Dokumente und Prozesse entsprechend anzupassen.

AUTOR

Michael Reinle, ist Partner und Mitglied der Praxisgruppe ICT & Digital von MLL Legal sowie Co-Head der Praxisgruppe Product Regulation. Er berät in- und ausländische Klienten vornehmlich bei Datenschutz-, IT-Vertrags- und Immaterialgüterrechtsfragen. Er verfügt über besondere Erfahrung bei komplexen Digitalisierungs- und IT-Entwicklungs- sowie Outsourcing-Projekten. Darüber hinaus berät er Klienten bei der Implementierung von neuen Technologien, inklusive AI-Anwendungen.