RUOSS VÖGELE PARTNER
RECHTSANWÄLTE ATTORNEYS AT LAW
RVP

RUOSS VÖGELE PARTNER | KREUZSTRASSE 54 | CH-8032 ZÜRICH
TELEFON +41 44 250 43 00 | FAX +41 44 250 43 10 | info@rvpartner.ch | www.rvpartner.ch

RVP Bulletin

Regelung des Datenschutzes im multinationalen Konzern (eine Übersicht)

Dr. Alois Rimle, LL.M.
rimle@rvpartner.ch

Zürich, Februar 2014, Nr. 1

Inhalt

Bearbeitung von Personendaten im Konzern

Beschreibung der Datenbearbeitung

Bevor in einem Konzern bestimmt werden kann, welche datenschutzrechtlichen Regeln anwendbar sind und wie sie konzernintern umgesetzt werden können,

muss der relevante Sachverhalt festgestellt werden. Je nach Geschäftstätigkeit des Unternehmens werden bestimmte Arten von Personendaten auf spezifische Weise bearbeitet.

Die Datenbearbeitung im Konzern muss auf angemessene Weise beschrieben werden. Diese Beschreibung umfasst hauptsächlich folgende Elemente:

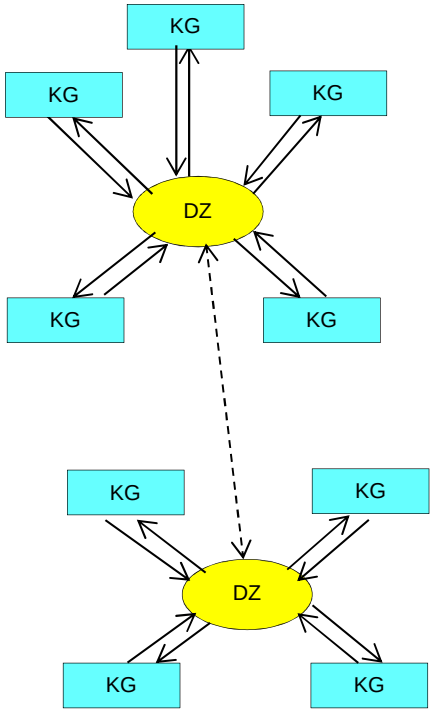
- „Group Chart“ mit Länderangaben;
- Geschäftsfunktionen und -organisation;
- IT-Infrastruktur (Datenzentren und Server-Standorte);
- Datenbearbeitungsprozesse;
- Arten der betroffenen Personen und Personendaten;
- Datenfluss mit Dateneingabe und -zugriff;
- Auslagerung der Datenbearbeitung (Cloud).

IT-Infrastruktur und Applikationen

Bei der elektronischen Bearbeitung von Personendaten im Konzern kann zwischen Datenzentrum (IT-Infrastruktur), Plattform (Anwendung) und Software (Applikations-Software) unterschieden werden:

- *Datenzentrum:* Konzerne mit internationaler Geschäftstätigkeit betreiben regelmässig regionale oder globale Datenzentren. Diese umfassen Server, auf denen die Gruppengesellschaften ihre Daten oder Anwendungen abspeichern können. Die IT-Infrastruktur betrifft das Netz, den Zugang zum Netz, die Hardware etc. Dabei umfassen Datenzentren regelmässig operative Server an einem Standort und Back-up-Server an einen geographisch getrennten anderen Standort. Sie enthalten zudem ein Sicherheitsdispositiv für wesentliche nicht voraussehbare Notfälle.
- *Plattform:* Im Datenzentrum wird eine Plattform (Anwendung) für die Datenbearbeitung entwickelt und zur Verfügung gestellt.
- *Software:* Es bedarf Applikations-Software, um die Daten mittels der Plattform bewirtschaften zu können.

Ein multinationaler Konzern betreibt (neben lokalen Servern) für gewöhnlich ein oder mehrere Datenzentren. Dabei sind die Konzerngesellschaften regelmässig einem spezifischen regionalen oder globalen Datenzentrum angeschlossen. Zwischen den verschiedenen Datenzentren findet möglicherweise ein beschränkter Datenaustausch statt. Datentransfers über Datenzentren eines Konzerns können vereinfacht wie folgt dargestellt werden:



Dokumentierung und Aktualisierung

Die Beschreibung der Datenbearbeitung in einem Konzern muss dokumentiert werden. Insbesondere sollte ein Inventar der verschiedenen konzerninternen Datenbearbeitungsprozesse erstellt werden. Zudem müssen Listen von Datensammlungen für jene Gruppengesellschaften erstellt werden, die nach lokalem Datenschutzrecht einer entsprechenden Meldepflicht unterstehen.

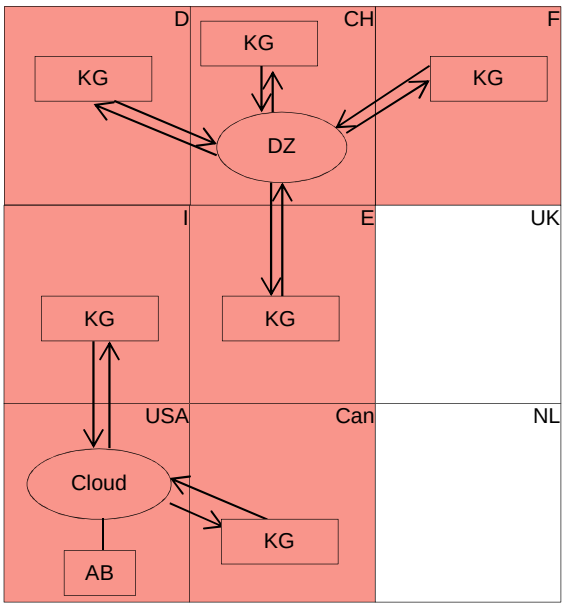
Die Datenbearbeitungsprozesse in einem Konzern sind in stetigem Fluss. Bestehende Bearbeitungsprozesse werden geändert und neue eingeführt. Aus diesem Grund ist es in einem Konzern erforderlich, dass die bestehende Dokumentation der gruppen-

weiten Datenbearbeitung regelmässig angepasst wird.

Anwendbare Datenschutzrechte

Datenschutzrecht ist hauptsächlich nationales Recht. Welche nationalen Datenschutzrechte auf die Datenbearbeitung in einem Konzern zur Anwendung kommen, bestimmt sich danach, wo Personendaten bearbeitet werden. Grundsätzlich findet die Datenbearbeitung dort statt, wo Gruppengesellschaften ihre Geschäftstätigkeit ausüben und wo Datenzentren betrieben werden. Ob ein bestimmtes Datenschutzgesetz anwendbar ist, bestimmt sich anhand von dessen Geltungsbereich.

Ein multinationaler Konzern hat seine Geschäftstätigkeiten in einer Vielzahl von Ländern. Er muss dementsprechend verschiedene Datenschutzrechte beachten. Dies kann vereinfacht wie folgt dargestellt werden:

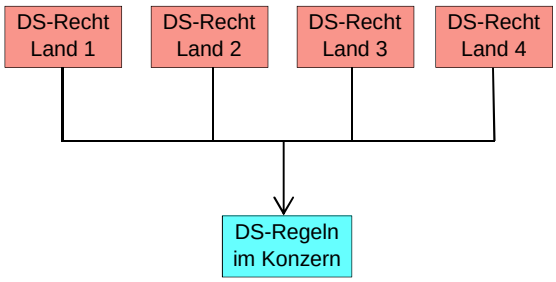


Die Bestimmungen in nationalen Datenschutzgesetzen sind im Wesentlichen privat-, verwaltungs- oder strafrechtlicher Natur. Ihre Anwendung auf die konzernweite Datenbearbeitung ist je nach Qualifizierung unterschiedlich:

- *Privatrechtliche Bestimmungen:* Die privatrechtlichen Bestimmungen (insbesondere die Bearbeitungsgrundsätze) sind in verschiedenen Ländern für gewöhnlich ähnlich ausgestaltet. Wenn bei ihnen ein hoher Standard auf der Grundlage der gesetzlichen Bestimmungen eines Landes mit angemessenem Datenschutz zur Anwendung gebracht wird, kann grundsätzlich davon ausgegangen werden, dass dieser Standard auch den gesetzlichen Anforderungen in den anderen relevanten Ländern entspricht. Ausnahmsweise bestehen in einzelnen Ländern Sondervorschriften, die länderspezifisch beachtet werden müssen. Solche Regeln bestehen etwa für Deutschland im Bereich des Datentransfers oder für Spanien im Bereich der Datensicherheit.
- *Verwaltungsrechtliche Bestimmungen:* Die verwaltungsrechtlichen Bestimmungen (insbesondere die Meldepflichten) müssen in jedem relevanten Land separat bestimmt und erfüllt werden.
- *Strafrechtliche Bestimmungen:* Die Strafbestimmungen in nationalen Datenschutzgesetzen werden regelmässig an die Verletzung von verwaltungsrechtlichen Bestimmungen anknüpfen. Sie müssen gegebenenfalls in jedem Land separat beachtet werden. Soweit sie hingegen an die Verletzung privatrechtlicher Bestimmungen anknüpfen, dürfte die Strafbarkeit mit der Umsetzung eines hohen Datenschutzstandards regelmässig vermieden werden können.

Rechtsumsetzung im Konzern

Es ist praktisch nicht möglich, dass Konzerne nationale Datenschutzrechte direkt auf ihre interne Bearbeitung von Personendaten anwenden. Zudem verlangen Datenschutzrechte regelmässig, dass die gesetzlichen Datenschutzbestimmungen durch konzerninterne Regeln basierend auf Richtlinien, Reglementen und Verträgen umgesetzt werden. Diese Umsetzung von anwendbaren Datenschutzrechten in einem multinationalen Konzern kann vereinfacht wie folgt dargestellt werden:



Datenschutz-Folgeabschätzungen

Wenn ein neues System oder ein neuer Datenbearbeitungsprozess mit höheren Datenschutzrisiken in einem Konzern eingeführt werden soll, muss grundsätzlich vorgängig eine Datenschutz-Folgeabschätzung durchgeführt werden. Sie dient der Erkennung von Datenschutzrisiken und erlaubt es früh im Erarbeitungsprozess eines Projekts, diejenigen Punkte zu identifizieren, die aus Datenschutzsicht heikel sind. Sowohl in der Schweiz als auch in der EU bestehen entsprechende Evaluationsraster. Anhand des Ergebnisses einer Folgeabschätzung kann das Projekt unter Berücksichtigung datenschutzrechtlicher Erfordernisse ausgestaltet werden.

Datenschutzrechtliche Massnahmen

Sparsame Beschaffung von Personendaten

Es ergibt sich aus dem Grundsatz der Verhältnismässigkeit, dass ein Unternehmen an sich nur solche Personendaten beschaffen darf, die es für die eigene Geschäftstätigkeit tatsächlich benötigt. Es darf keine Daten auf Vorrat beschaffen. Ein Unternehmen, das systematisch unnötige Personendaten beschafft, verhält sich datenschutzrechtswidrig.

Vor diesem Hintergrund empfiehlt es sich für Unternehmen, die Beschaffung von Personendaten bewusst zu steuern. Beispielsweise sollte für den HR-Bereich definiert und dokumentiert werden, welche Arten von Informationen von welchen Kategorien von Mitarbeitenden beschafft werden dürfen und welche nicht. Dasselbe gilt für die Beschaffung von Kundendaten. Zudem sollten Prozesse für die Vernichtung bzw. Löschung von nicht mehr benötigten (und unnötigerweise beschafften) Personendaten etabliert werden.

Insbesondere die Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen sollte möglichst vermieden oder eingeschränkt werden. Die Bearbeitung solcher Informationen unterliegt nämlich nach den Datenschutzrechten von Ländern mit angemessenem Datenschutz zusätzlichen Einschränkungen und Anforderungen (z.B. Einwilligungserfordernis).

Umgang mit privaten Informationen

Unternehmen dürfen grundsätzlich keine privaten Informationen von Mitarbeitenden oder Kunden bearbeiten. Gleichwohl lässt sich eine solche Datenbearbeitung im Unternehmen nicht ganz vermeiden. Beispielsweise senden oder erhalten Mitarbeitende private E-Mails, die in der Folge auf dem E-Mail-Server des Unternehmens gespeichert werden. Mitarbeitende legen private Informationen auf der Festpatte des eigenen Computers ab. Kunden stellen dem Unternehmen auf dessen Website private Informationen zur Verfügung.

Da Unternehmen die Bearbeitung privater Informationen möglichst vermeiden müssen, erscheint es sinnvoll, intern ein Konzept für den Umgang mit privaten Informationen zu entwickeln. Dabei sollten insbesondere folgende Einschränkungen beachtet werden: Die Speicherung privater Informationen sollte möglichst beschränkt werden. Im Weiteren dürfen gespeicherte private Informationen nur sehr limitiert in Überwachungsmassnahmen (z.B. E-Mail- oder Internet-Überwachung) einbezogen werden (siehe Anleitungen von Datenschutzbehörden in relevanten Ländern). Schliesslich haben die betroffenen Personen grundsätzlich einen Anspruch auf Löschung ihrer privaten Informationen und können diesen nach Massgabe des anwendbaren Datenschutzrechts auch gegen das Unternehmen rechtlich durchsetzen.

Umwandlung in Nicht-Personendaten

Datenschutzrechtliche Anforderungen greifen nur ein, wenn Personendaten bearbeitet werden. Wenn Daten bearbeitet werden, die keine Personendaten sind, müssen auch keine datenschutzrechtlichen Anforderungen beachtet werden. Als Personendaten gelten etwa nach schweizerischem Datenschutzrecht „alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen“ (Art. 3 Abs. 1 lit. a DSG) oder nach der EU-Datenschutzrichtlinie „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“ (Art. 2 lit. a).

Das Schweizerische Bundesgericht hält in diesem Zusammenhang Folgendes fest: „Bestimmbar ist die Person, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat." (BGE 136 II 508, 514). „Ob eine Information aufgrund zusätzlicher Angaben mit einer Person in Verbindung gebracht werden kann, sich die Information mithin auf eine bestimmbare Person bezieht (Art. 3 lit. a DSG), beurteilt sich aus der Sicht des jeweiligen Inhabers der Information." (BGE 136 II 508, 515).

Wenn man davon ausgeht, dass in anderen Ländern vergleichbare Regeln für die Bestimmbarkeit von Personen gelten, ist es in einem Konzern möglich, Personendaten für bestimmte Bearbeitungsschritte oder deren Aufbewahrung gewissermassen in Nicht-Personendaten umzuwandeln, sodass im entsprechenden Umfang kein Datenschutzrecht zur Anwendung kommt. Wenn beispielsweise anonymisierte oder pseudonymisierte Daten an einen Dienstleister im Ausland (ohne Befugnis zum Weitertransfer) weitergeleitet werden und dieser zur Re-Identifikation nicht in der Lage ist, liegen aus dessen Sicht mangels Personenbezugs keine Personendaten vor. Gegebenenfalls müssen die datenschutzrechtlichen Anforderungen an den Datentransfer in Länder ohne angemessenen Datenschutz nicht beachtet werden. Dasselbe gilt, wenn elektronische Personendaten (d.h. Programme) gewissermassen „aufgesplittet" werden oder unter Umständen auch dann, wenn Personendaten vollständig verschlüsselt werden.

Mehr ist besser als weniger

Es ist m.E. nicht korrekt zu sagen, dass die Datenbearbeitung in einem Konzern insgesamt entweder datenschutzkonform oder nicht datenschutzkonform ist. Es ist zutreffender zu sagen, dass die Datenbearbeitung in einem Konzern mehr oder weniger, aber gewiss nie 100% datenschutzkonform ist. Die Bearbeitung von Personendaten kann und sollte in einem Konzern deshalb auf der Grundlage datenschutzrechtlicher Anforderungen regelmässig überprüft und angepasst bzw. verbessert werden.

Risikobasierter Ansatz

Einige Bearbeitungssysteme im Konzern werden viele Personendaten (z.B. HR-Systeme), andere kaum Personendaten enthalten. Zudem sind Personendaten nicht gleich Personendaten. Beispielsweise wiegt eine unzulässige Offenlegung von besonders schützenswerten Personendaten aus persönlichkeitsrechtlicher Sicht schwerer als jene von einfachen Personendaten.

Es ist deshalb wichtig, jene Bearbeitungsprozesse in einem Konzern zu identifizieren, in denen viele oder heikle Personendaten, insbesondere besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden. Die datenschutzrechtlichen Massnahmen sollten sich zuerst auf diese Bearbeitungsprozesse beziehen.

Sicherheit und Aufbewahrung in Datenzentren

Datenzentren machen in einem Konzern nicht nur aus Effizienz- und Kostengründen Sinn. Sie sind für gewöhnlich auch in der Lage, ein erheblich höheres Datensicherheitsniveau zu gewährleisten, als dies bei lokalen Servern möglich wäre. Die Datenbearbeitung in regionalen oder globalen Datenzentren ist somit auch aus Sicht des Datenschutzrechts zu begrüssen.

Datenzentren dienen neben der Datenspeicherung auch der elektronischen Aufbewahrung von Dokumenten. Sie umfassen nicht nur strukturierte Datenbanken, sondern auch Systeme zur elektronischen Aufbewahrung von Dokumenten und E-Mails (Dokumenten- und E-Mail-Speichersysteme). Die elektronische Aufbewahrung von Dokumenten kann so ausgestaltet werden, dass die gesetzlichen Aufbewah-

rungsanforderungen in den betroffenen Ländern mehrheitlich oder gar vollständig erfüllt sind, sodass alle oder die meisten Dokumentenarten nicht länger in Papierform aufbewahrt werden müssen.

Die elektronische Aufbewahrung von Daten und Dokumenten wird gelegentlich auf mögliche Offenlegungspflichten ausgerichtet. Beispielsweise kann die Speicherung von E-Mails im Hinblick auf eine konzernweite Datenoffenlegung im Rahmen einer „Pre-Trial Discovery" insbesondere in den USA spezifiziert vorgenommen werden.

Es sollte in diesem Zusammenhang schliesslich erwähnt werden, dass bei der Aufbewahrung von Daten und Dokumenten in regionalen oder globalen Datenzentren allenfalls auch aufsichtsrechtliche Anforderungen und Einschränkungen beachtet werden müssen, wenn regulierte Geschäftstätigkeiten betroffen sind. Gegebenenfalls können Datenzentren aufsichtsrechtlich als Fälle von IT-Auslagerung gelten, die den Aufsichtsbehörden in den betroffenen Ländern gemeldet oder von diesen gar genehmigt werden müssen.

Datenschutzkonforme Produkte

Applikationen sind möglichst unter Berücksichtigung des Datenschutzrechts auszugestalten. Nach schweizerischem Datenschutzrecht (Art. 5 VDSZ) können Produkte, deren eigentlicher Zweck die Datenbearbeitung ist, und Produkte, bei deren Benutzung Personendaten anfallen, grundsätzlich zertifiziert werden. Im Rahmen einer solchen Zertifizierung wird die produktimmanente Gewährleistung verschiedener datenschutzrelevanter Aspekte beurteilt.

Standardmässige Transparenz

Betroffene Personen müssen wissen bzw. erkennen können, dass ein Unternehmen Daten über sie bearbeitet, damit sie ihre Rechte wahrnehmen können. Daraus ergibt sich regelmässig eine datenschutzrechtliche Pflicht für Unternehmen, die betroffenen Personen über die Beschaffung und Bearbeitung ihrer Daten zu informieren. Dieser Grundsatz gilt nicht nur im schweizerischen, sondern auch in anderen Datenschutzrechten.

Unternehmen sollten ihre Mitarbeitenden, Kunden und Lieferanten, soweit rechtlich erforderlich, standardmässig und möglichst auf Konzernstufe über die Bearbeitung ihrer Daten informieren. Dies kann mittels Vertragsklauseln, separaten Mitteilungen, Mitteilungen auf der Website oder auf andere Weise geschehen.

Identifizierung von Einwilligungsfällen

Die Einwilligung ist ein problematischer Rechtfertigungsgrund für die Bearbeitung von Personendaten: Erstens sind die Anforderungen an eine datenschutzrechtlich gültige Einwilligung hoch. Wird die Einwilligung unkorrekt verwendet, stellt sie keine geeignete Grundlage für die Datenbearbeitung dar. Zweitens vermag die Einwilligung keinen Rechtfertigungsgrund für die Datenbearbeitung zu liefern, wenn sie im Rahmen eines klaren Ungleichgewichts zwischen Datenverantwortlichem und betroffener Person erteilt wird (z.B. Einwilligungsfälle im Arbeitsverhältnis). Drittens ist die Einwilligung ein instabiler Rechtfertigungsgrund für die Datenbearbeitung, indem sie jederzeit zurückgezogen werden kann.

Die Einwilligung ist einer von mehreren datenschutzrechtlichen Rechtfertigungsgründen für die Bearbeitung von Personendaten. In einem Konzern sollte die Einwilligung nur verwendet werden, wenn für eine notwenige Datenbearbeitung kein anderer Rechtfertigungsgrund zur Verfügung steht. Insbesondere eignet sich die Einwilligung von Mitarbeitenden und Kunden für standardmässige Bearbeitungsprozesse grundsätzlich nicht, wenn keine Bearbeitungsalternative für den Fall des Widerrufs der Einwilligung vorhanden ist. Dagegen eignet sich die Einwilligung für die Rechtfertigung von spezifischen und einmaligen Bearbeitungsfällen (z.B. Zustimmung des Mitarbeitenden zu psychologischem Test in Promotionsverfahren).

Es erscheint sinnvoll, die konzernweite Datenbearbeitung auf ihre Rechtfertigungsgründe hin zu untersuchen und jene Fälle zu identifizieren, bei denen die Einwilligung der betroffenen Person erforderlich ist. Für diese Fälle kann in der Folge eine schriftliche Standard-Einwilligungserklärung abgefasst und verwendet werden, die aus datenschutzrechtlicher Sicht gültig ist.

Datenschutz-Governance

Effektive Umsetzung im Konzern

Konzerne müssen praktische Massnahmen ergreifen, um anwendbare Datenschutzrechte effektiv umzusetzen. Dabei stehen insbesondere folgende Massnahmen im Vordergrund: Abschluss von Datentransferverträgen, Erlass von Richtlinien und Reglementen, Ernennung von verantwortlichen Personen, Durchführung von Datenschutzkursen sowie Festlegung von Datenschutzprozessen und Compliance-Massnahmen. Der Datenschutz sollte in einem multinationalen Konzern mehrheitlich zentral organisiert werden, insbesondere weil konzerninterne Datenbearbeitungsprozesse gleichzeitig mehreren Datenschutzrechten mit vergleichbaren Regeln unterstehen.

Verantwortliche Personen

Es erscheint notwendig, auf Konzernstufe eine verantwortliche Person für den Datenschutz und eine verantwortliche Person für die Datensicherheit zu ernennen. Je nach den Verhältnissen im Einzelfall können diese Funktionen zusammengelegt und mit anderen Funktionen kombiniert werden. Den verantwortlichen Personen sollten erhebliche Kompetenzen im Bereich des Datenschutzes und der Datensicherheit eingeräumt werden, geht es dabei doch überwiegend um „technische“ Fragen, die an Legal & Compliance oder IT gerichtet sind und die zudem rasch und flexible beantwortet werden und zu effizienten Massnahmen führen müssen. Im Weiteren kann es auf der Stufe der Länder oder Gruppengesellschaften gesetzlich vorgeschrieben sein, einen lokalen Datenschutzverantwortlichen einzusetzen.

Datenschutzausbildung

Die Mitarbeitenden eines Konzerns, die im Rahmen ihrer Aufgaben Personendaten bearbeiten (z.B. HR-Personal), müssen von Zeit zu Zeit im Datenschutzrecht aus- und weitergebildet werden. Nur dann sind sie auch in der Lage, bestehende Konzernrichtlinien und Bearbeitungsreglemente in ihren jeweiligen Verantwortungsbereichen anzuwenden.

Datenschutzprozesse

Folgende Datenschutzprozesse sollten in multinationalen Konzernen grundsätzlich aufgesetzt werden:

- Prozess, um Zugriffs-, Berichtigungs- und Löschungsbegehren von betroffenen Personen zu behandeln;
- Prozess, um Beschwerden von betroffenen Personen zu behandeln;
- Prozess, um mit Sicherheitsverstössen umzugehen und falls erforderlich diese zu melden;
- Prozess zur Durchführung von Datenschutz-Folgeabschätzungen unter spezifischen Umständen;
- Prozess zur Durchführung von Compliance-Massnahmen.

Compliance

Es sollte in einem Konzern periodisch verifiziert werden, dass die ergriffenen Datenschutzmassnahmen ausreichend sind, um die Bearbeitungsgrundsätze und andere datenschutzrechtliche Anforderungen effektiv umzusetzen. Dies kann etwa dadurch bewerkstelligt werden, dass die verantwortlichen Personen Massnahmen kontrollieren und dass interne oder externe Audits durchgeführt werden. Auf diese Weise kann sichergestellt werden, dass die getroffenen Massnahmen nicht nur auf dem Papier bestehen, sondern im Konzern tatsächlich auch umgesetzt werden.

Verträge für gruppeninterne Datentransfers

Vertragserfordernis bei Datentransfers

In einem Konzern finden über gruppenweite Bearbeitungssysteme täglich unzählige Transfers von Personendaten statt. Solche Datentransfers machen es nach EU und schweizerischem Datenschutzrecht regelmässig erforderlich, dass schriftliche Datentransferverträge zwischen den betroffenen Gruppengesellschaften abgeschlossen werden.

Ein schriftlicher Datentransfervertrag ist für gewöhnlich notwendig, wenn Personendaten grenzüberschreitend aus einem EU-Staat oder der Schweiz in ein Land ohne angemessenen Datenschutz transferiert werden. Der Transfervertrag soll bei der Empfängergesellschaft einen angemessenen Datenschutz gewährleisten. Zu diesem Zweck stehen in der EU und der Schweiz geeignete Standard-Vertragsklauseln zur Verfügung. Ein schriftlicher Vertrag ist selbst für Datentransfers innerhalb der EU oder der Schweiz erforderlich, wenn eine Gesellschaft Personendaten im Auftrag einer anderen Gesellschaft bearbeitet (Auftragsdatenbearbeitung). Das Vertragserfordernis gilt auch für die entsprechenden Datentransfers zwischen Gruppengesellschaften eines Konzerns.

Vorbehalten bleibt der Fall, da in einem Konzern „Binding Corporate Rules" implementiert werden. Gegebenenfalls besteht ein reduzierter bzw. geänderter Bedarf nach bindenden Verträgen (siehe hinten).

Multilaterale Datentransferverträge

Es wäre kaum praktikabel, für alle Arten von Datentransfers in einem Konzern bilaterale Datentransferverträge zwischen betroffenen Gruppengesellschaften abzuschliessen. Deshalb drängt es sich auf, statt unzähliger bilateraler Transferverträge konzernweit nur einen oder wenige multilaterale Transferverträge abzuschliessen.

Multilaterale Verträge können etwa auf der Stufe der einzelnen Bearbeitungssysteme (z.B. HR-Datenbank, geschäftsspezifische Systeme, E-Mail-Server etc.) abgeschlossen werden. Bei diesem Ansatz dürften in einem grossen Konzern immer noch zahlreiche Verträge erforderlich sein. Es ist deshalb sinnvoll, einen einzigen multilateralen Vertrag für alle geschäftsbezogenen Datentransfers abzufassen. Ein solcher Vertrag ist gewiss umfassend und beinhaltet mehrere Anhänge zur Regelung der verschiedenen Geschäftsfunktionen und deren Bearbeitungssysteme. Es ist aber immer noch einfacher, einen einzigen komplizierten Vertrag zu handhaben als eine Vielzahl bilateraler oder systembezogener multilateraler Verträge zu verwalten. Neben einem solchen umfassenden geschäftsbezogenen Vertrag wird grundsätzlich nur noch ein multilateraler Vertrag für HR-bezogene Datentransfers erforderlich sein.

„Ring fencing" auf tiefem Schutzniveau

Aus Sicht der Datenschutzrechte der Schweiz und der EU gibt es einerseits Länder mit angemessenem Datenschutz (EU-Staaten, Schweiz, gewisse weitere Länder) und andererseits Länder ohne angemessenen Datenschutz. Soweit die Bearbeitung von Personendaten auf Länder beschränkt wird, die über keinen angemessenen Datenschutz verfügen, besteht auch keine Notwendigkeit, die weitergehenden datenschutzrechtlichen Anforderungen in Ländern mit angemessenem Datenschutz anzuwenden. Somit ist es für global tätige Konzerne grundsätzlich möglich, die konzerninterne Bearbeitung von Personendaten auf unterschiedlichen Niveaus zu betreiben. Beispielsweise kann die Datenbearbeitung in der Schweiz unter Beachtung hoher Anforderungen und jene in den USA unter Beachtung geringerer Anforderungen betrieben werden. Ob dies wünschbar ist, ist eine andere Frage. Viele Konzerne sind vielmehr bestrebt, ein gruppenweit einheitliches und hohes Datenschutzniveau umzusetzen und dieses an ihre Kunden und die Öffentlichkeit zu kommunizieren.

Die Bearbeitung von Personendaten auf tiefem Schutzniveau ist im Konzern nur zulässig, solange sie auf Länder ohne angemessenen Datenschutz beschränkt bleibt. Dabei ist es für Gruppengesellschaften in Ländern ohne angemessenen Datenschutz (z.B. USA) grundsätzlich immer noch möglich, ihre Personendaten auf einen zentralen Gruppenserver in einem Land mit angemessenem Datenschutz (z.B. Schweiz) zu transferieren, sie dort zu speichern und in der Folge auf sie online zuzugreifen. Soweit dabei nur Mitarbeitende in den Ursprungsländer vorgängig transferierte Personendaten bearbeiten, müssen die betreffenden Gruppengesellschaften m.E. deswegen nicht zu einem höheren Datenschutzniveau verpflichtet werden. Anders verhält es sich hingegen grundsätzlich mit Personendaten, die nicht vorgängig transferiert wurden, sondern im Rahmen der Datenbearbeitung im Gruppensystem neu bzw. zusätzlich geschaffen wurden. Auf die Bearbeitung solcher Daten wird an sich der höhere Datenschutzstandard anwendbar sein („Infizierung durch höheres Datenschutzniveau").

Konzernrichtlinien und Reglemente

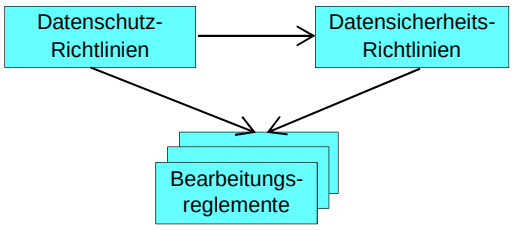
Regelungsarchitektur im Konzern

Im Interesse eines effektiven Datenschutzes im Konzern ist es entscheidend, dass die zuständigen Mitarbeitenden angemessen angewiesen werden, wie Personendaten rechtskonform zu bearbeiten sind. Dies betrifft nicht nur die Mitarbeitenden in Ländern mit angemessenem Datenschutz, sondern auch jene in Ländern ohne angemessenen Datenschutz. Die dortigen Arbeitgeber-Gruppengesellschaften haben sich nämlich durch gruppeninterne Datentransferverträge zur Einhaltung eines angemessenen Datenschutzes verpflichtet (siehe vorne).

Es stellt sich die Frage, wie Mitarbeitende, die Personendaten bearbeiten, im Konzern am besten informiert und instruiert werden können. Datenschutzrechtliche Informationen und Instruktionen zuhanden von Mitarbeitenden erfolgen grundsätzlich auf dem Weg von Richtlinien und Reglementen.

Es müssen zunächst vom zuständigen Gremium konzernweite Datenschutzrichtlinien und Datensicherheitsrichtlinien erlassen werden. Übergeordnete Konzernrichtlinien sind zwar erforderlich, helfen dem einzelnen bearbeitenden Mitarbeitenden beim konkreten Umgang mit Personendaten in seinem Arbeitsbereich aber kaum. Wenn in der Datenschutzrichtlinie beispielsweise steht, Personendaten seien verhältnismässig zu bearbeiten, so dürfte der einzelne Mitarbeitende oftmals nicht in der Lage sein, zu bestimmen, was Verhältnismässigkeit im konkreten Einzelfall bedeutet. Aus diesem Grund müssen die Konzernrichtlinien für die wichtigen Bearbeitungsfälle mittels geeigneter Bearbeitungsreglemente (z.B. HR-Bearbeitungsreglement) konkretisiert werden.

Die Architektur der datenschutzrechtlichen Richtlinien und Reglemente in einem Konzern können vereinfacht wie folgt dargestellt werden:



Die in einem Konzern bestehenden datenschutzrechtlichen Richtlinien und Bearbeitungsreglemente richten sich hauptsächlich an die Mitarbeitenden, die Personendaten bearbeiten. Sie müssen deshalb (anders als Datentransferverträgen) möglichst einfach und verständlich abgefasst sein.

Datenschutzrichtlinien auf Konzernstufe

Die Datenschutzrichtlinien auf Konzernstufe enthalten lediglich eine datenschutzrechtliche Rahmenordnung. Sie regeln u.a. die Bearbeitungsgrundsätze und Aspekte der Datenschutz-Governance. Sie können für gruppenweite Detailregelungen auch auf separate Richtlinien verweisen und dabei Kompetenzen delegieren (z.B. Regelung erforderlicher Bearbeitungsprozesse).

Datensicherheitsrichtlinien auf Konzernstufe

IT-spezifische Risiken müssen mit einem effizienten Risikomanagement bewirtschaftet werden. Ein solches Risikomanagement ist über eine klar definierte IT-Governance und eine sich daran orientierende IT-Sicherheitsstrategie zu erreichen. Die IT-Governance umfasst die Steuerung und Kontrolle von Risiken sowie die Spezifizierung von Verantwortlichkeiten in der Informationstechnologie. Die IT-Sicherheitsstrategie legt die Sicherheitsprinzipien und Sicherheitsziele fest.

Die Inhalte der IT-Governance und Informationssicherheit sind in international anerkannten Rahmenwerken (Selbstregulierungs-Standards) festgelegt (z.B. ISO 2700X). Ausgehend von den Inhalten dieser internationalen Rahmenwerke und den gesetzlichen Vorgaben in den betroffenen Ländern ist eine Informationssicherheitsrichtlinie zu erlassen, um die IT-Governance, die IT-Sicherheitsstrategie und deren Umsetzung zu regeln. Geregelt werden schliesslich etwa auch das Reporting und die Anpassung an veränderte Verhältnisse.

Bearbeitungsreglemente

Im Konzern gibt es regelmässig eine Vielzahl von verschiedenen Datenbearbeitungsfällen, bei denen sich jeweils spezifische datenschutzrechtliche Fragen stellen. Es ist deshalb datenschutzrechtlich erforderlich, die wichtigen Datenbearbeitungsprozesse zu regeln. Dabei geht es nicht nur um Prozesse im HR-

Bereich (z.B. Anstellungsprozess, Internet- und E-Mail-Überwachung, Video- und GPS-Überwachung etc.). Jedes wichtige Bearbeitungssystem mit einem spezifischen Zweck kann besondere Regeln erforderlich machen, wenn darin Personendaten bearbeitet werden. Diesbezüglich enthält beispielsweise das schweizerische Datenschutzrecht eine grundsätzliche Pflicht zur Erstellung eines Bearbeitungsreglements für jede automatisierte Datensammlung, bei der regelmässig Personendaten an Dritte bekannt gegeben werden oder regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden (Art. 11 Abs. 1 VDSG).

Es erscheint m.E. aus verschiedenen Gründen sinnvoll, die Kompetenz zum Erlass spezifischer Bearbeitungsreglemente an den Datenschutzverantwortlichen des Konzerns zu delegieren: Dieser ist fachlich in der Lage, zu entscheiden, wo ein Bearbeitungsreglement erforderlich ist und welche Regeln gegebenenfalls in einem Bearbeitungsreglement enthalten sein müssen. Im Weiteren kann der Datenschutzverantwortliche auf laufende Veränderungen bei der Datenbearbeitung im Konzern reagieren und einmal erlassene Bearbeitungsreglemente nötigenfalls auch rasch wieder ändern. Dies liegt ganz im Interesse eines effektiven Datenschutzes im Konzern.

Binding Corporate Rules

BCRs als genehmigtes Gesamtkonzept

Die Verwendung von Binding Corporate Rules (BCRs) als rechtliche Grundlage für den grenzüberschreitenden Datentransfer innerhalb des Konzerns macht es nach EU-Recht erforderlich, dass von den „Data Controllers“ im Konzern angemessene Schutzmassnahmen ergriffen werden. Auf der Grundlage solcher Schutzmassnahmen und deren Dokumentierung werden dann die grenzüberschreitenden Datentransfers in einem besonderen EU-Verfahren unter der Verantwortung eines „Lead Regulators“ genehmigt. Die BCRs umfassen verschiedene interne Massnahmen, um die Bearbeitungsgrundsätze im Konzern umzusetzen (z.B. Ernennung von verantwortlichen Personen, Festlegung von Prozessen, Durchführung der Ausbildung, Erlass von Richtlinien). Diese konzernweiten internen Massnahmen dienen letztlich der Umsetzung der vertraglichen Gewährleistung des angemessenen Datenschutzes beim grenzüberschreitenden Datentransfer in Länder ohne angemessenen Datenschutz.

Die Genehmigung von BCRs steht auch Konzernen mit Sitz in der Schweiz und Tochtergesellschaften in der EU offen. Schweizerische Konzerne können das Verfahren grundsätzlich vor der Datenschutzbehörde eines EU-Staates einleiten, in dem sie geschäftlich tätig sind. Sind die BCRs in der EU einmal genehmigt worden, müssen sie noch dem Schweizerischen Datenschutz- und Öffentlichkeitsbeauftragten mitgeteilt werden (Art. 6 Abs. 2 lit. g und Abs. 3 DSG; Art. 6 Abs. 1 VDSG).

Inhalt von BCRs

Die BCRs (in einem weiten Sinn verstanden) stellen ein Gesamtkonzept für die Regelung des Datenschutzes in einem Konzern dar und umfassen alle genehmigten und dokumentierten Massnahmen. Sie umfassen insbesondere folgende Arten von Dokumenten:

- Genehmigungsgesuch mit Erklärungen und Beschreibungen der Bearbeitungssysteme und Datenflüsse;
- BCRs (in einem engen Sinn verstanden) als übergeordnete Datenschutzrichtlinien, allenfalls mit Anhängen;
- Richtlinien und Reglemente, welche insbesondere auch die Datenschutzprozesse umschreiben;
- erforderliche konzerninterne Transferverträge;
- Informationsdokumente (Transparenz);
- Erfüllung spezifischer Anforderungen gemäss nationaler Datenschutzrechte (z.B. Meldepflichten).

Genehmigte BCRs oder eigenständige Massnahmen

Ein Konzern muss nicht unbedingt BCRs genehmigen lassen, um eine grundsätzlich rechtskonforme interne Bearbeitung von Personendaten sicherzustellen. Er kann dies auch eigenständig ohne behördliche Genehmigung bewerkstelligen, indem er multila-

terale Verträge abschliesst und zusätzlich Richtlinien und Reglemente erlässt und diese umsetzt. Es besteht für den Konzern somit eine Wahl zwischen behördlich genehmigten BCRs und eigenständig umgesetzten Datenschutzmassnahmen. Bei beiden Ansätzen sind die erforderlichen Massnahmen und Dokumente vergleichbar. Allerdings sind die vertraglichen Anforderungen bei BCRs teilweise anders und geringfügiger als bei eigenständig umgesetzten Datenschutzmassnahmen.

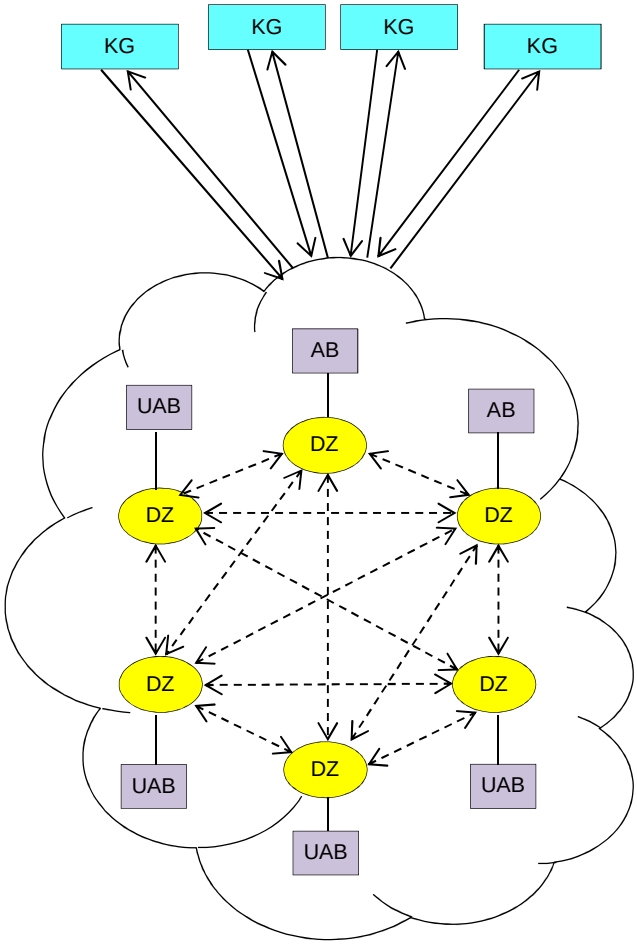
Cloud Computing

Externe Auftragsdatenbearbeitung

Es erscheint für einen Konzern insbesondere aus Kostengründen sinnvoll, einen Teil der Datenbearbeitung durch einen spezialisierten Dienstleister in einer Cloud durchführen zu lassen. Dabei ist die sogenannte „Public Cloud“ gemeint, bei der die Infrastruktur vollständig durch einen externen Cloud-Anbieter bewirtschaftet und bestimmt wird. Der Cloud-Nutzer hat insbesondere keinen Einfluss auf die Server-Standorte.

Cloud Computing besteht aus einer Reihe von Technologien und Servicemodellen, die sich auf den internetbasierten Gebrauch und die internetbasierte Lieferung von IT Applikationen, Verarbeitungsfähigkeiten sowie Aufbewahrungs- und Speicherkapazitäten beziehen. Der Service kann in der blossen Infrastruktur bestehen, wobei der Cloud-Anbieter in der Cloud einen Server zur Verfügung stellt, auf dem die Cloud-Nutzer ihre Daten und Anwendungen abspeichern können („Infrastructure as a Service (IaaS)“). Im Weiteren kann der Cloud-Anbieter eine Anwendung entwickeln und diese den Nutzern in der Cloud zwecks Datenbewirtschaftung zur Verfügung stellen („Platform as a Service (PaaS)“). Schliesslich kann der Cloud-Anbieter auch die Bewirtschaftung der Daten mittels geeigneter Software übernehmen, sodass der Cloud-Nutzer nur noch Konsument in der Cloud ist, dem eine Funktionalität zur Verfügung gestellt wird, um dort Daten bearbeiten zu können („Software as a Service (SaaS)“).

Cloud Computing-Dienstleistungen können den Einbezug von mehreren Vertragsparteien als Auftragsdatenbearbeiter umfassen. Im Weiteren ist es üblich, dass Auftragsdatenbearbeiter zusätzliche Unterauftragsdatenbearbeiter beauftragen, die Zugriff auf Personendaten erhalten. Es kann in einer Cloud in der Folge zu einer Vielzahl von Datentransfers zwischen Servern bzw. Datenzentren von Auftrags- und Unterauftragsbearbeitern kommen. Die Bearbeitung von Personendaten in einer Cloud im Auftrag von Konzerngesellschaften kann vereinfacht wie folgt dargestellt werden:



Risiko und Risikoanalyse

Die Datenschutz-Risiken im Zusammenhang mit Cloud Computing betreffen vor allem die mangelnde Kontrolle über die Personendaten und die ungenü-

gende Information darüber, wie, wo und durch wen die Daten bearbeitet oder unterbearbeitet werden.

Datenschutzrechtlich handelt es sich bei der Beziehung zwischen Cloud-Kunde und Cloud-Anbieter in der Regel um eine Controller-Processor-Beziehung. Das Unternehmen, das Personendaten in eine Cloud transferiert, ist für die Einhaltung des Datenschutzrechts verantwortlich. Es muss deshalb einen Cloud-Anbieter auswählen, der die Einhaltung des anwendbaren Datenschutzrechts gewährleistet, und sicherstellen, dass die rechtlichen Anforderungen auch tatsächlich umgesetzt werden. Dies betrifft nicht nur den Aspekt der Datensicherheit, sondern auch die verschiedenen datenschutzrechtlichen Pflichten (z.B. Beachtung von Zweckbestimmung, Verhältnismässigkeit, Transparenz etc.).

Im Ergebnis muss das Unternehmen vor der Beauftragung eines Cloud-Anbieters eine datenschutzrechtliche Risikoanalyse durchführen. Es muss sich überlegen, welche Anwendungen und Daten es am eigenen Standort behalten will und welche in die Cloud wandern sollen und gegebenenfalls welche Cloud für die Datenbearbeitung geeignet ist. Bei den Cloud-Anbietern wird man insbesondere zwischen solchen unterscheiden, die eine Datenbearbeitung in der Schweiz bzw. der EU garantieren, und solchen, die eine entsprechende Garantie nicht abgeben. Dabei wird man allenfalls auch das Risiko der Datenüberwachung im Fall von US-Anbietern bzw. Serverstandorten in den USA einbeziehen.

Verträge und Processor-BCRs für die Cloud

Cloud Computing basiert regelmässig auf dem vollständigen Fehlen eines stabilen Datenstandorts innerhalb des Netzwerkes des Cloud-Anbieters. Dabei können Daten um 3 Uhr in einem Datenzentrum und um 6 Uhr in einem anderen Datenzentrum auf der anderen Seite der Welt sein. Vor diesem Hintergrund stossen die herkömmlichen Mittel, den Datentransfer in Länder ohne angemessenen Datenschutz zu regeln, an Grenzen.

Eine Regelungsmöglichkeit besteht darin, im Vertrag zwischen dem Unternehmen und dem Cloud-Anbieter in einem Land ohne angemessenen Datenschutz die Standard-Klauseln zu verwenden und falls nötig anzupassen (wobei die Klauseln dann nicht mehr als Standard-Klauseln gelten können). Wenn der Cloud-Anbieter seinen Sitz in einem Land mit angemessenem Datenschutz hat, kann die Situation komplizierter werden, weil die Standardklauseln dann nicht anwendbar sind. Was die vertragliche Beziehung zwischen dem Auftragsbearbeiter in einem Land ohne angemessenen Datenschutz und einem Unterauftragsbearbeiter betrifft, so sollte ein schriftlicher Vertrag abgeschlossen werden, der dieselben Pflichten des Unterauftragsbearbeiters vorsieht, die gemäss Standardklauseln auch für den Auftragsbearbeiter gelten.

Eine Regelungsalternative bieten in der EU die 2012 und 2013 von der Artikel-29-Datenschutzgruppe entwickelten Processor-BCRs, die den Datentransfer innerhalb der Gruppe des Cloud-Anbieters (d.h. an Unterauftragsbearbeiter) im Interesse des Controllers erlauben, ohne dass dafür die Unterzeichnung von Verträgen zwischen Auftragsbearbeiter und Unterauftragsbearbeitern je Kunde erforderlich wäre. Der Inhalt der Processor-BCRs einer Processor-Gruppe muss vorgängig von den betreffenden Datenschutzbehörden in der EU genehmigt werden. Die genehmigten Richtlinien bilden in der Folge einen Anhang zum Dienstleistungsvertrag zwischen dem Cloud-Anbieter und dem jeweiligen Unternehmen (Kunde).

Abkürzungen

AB:	Auftragsdatenbearbeiter
BCRs:	Binding Corporate Rules
BGE:	Bundesgerichtsentscheid
DS:	Datenschutz
DSG:	Schweizerisches Bundesgesetz über den Datenschutz von 1992
DZ:	Datenzentrum
EDÖB:	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EU:	Europäische Union
KG:	Konzerngesellschaft oder Zweigniederlassung einer Konzerngesellschaft
VDSG:	Verordnung zum Bundesgesetz über den Datenschutz von 1993
UAB:	Unterdatenauftragsbearbeiter
VDSZ:	Verordnung über die Datenschutzzertifizierung von 2007

Auf www.rvpartner.ch verfügbare Bulletins und Broschüren in PDF-Form

2013

- Wettbewerbsabreden und Marktbeherrschung unter besonderer Berücksichtigung des schweizerischen Versicherungsmarktes (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Geschäftsraummiete
  Chasper Kamer, LL. M.
- Aufsichtsrechtliche Optimierung in der unabhängigen Vermögensverwaltung (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M
- Verantwortlichkeit und Haftung des Verwaltungsrats (eine Übersicht)
  (RVP)
- Umstrukturierungen im Versicherungskonzern (eine Übersicht)
  Dr. Alois Rimle, LL.M.
- Der Vorsorgeauftrag – Delegieren Sie Ihre Sorge(n)
  Bigna Grauer

2012

- Entwicklungen im Unternehmens- Datenschutzrecht der Schweiz und der EU im Jahr 2011
  Dr. Alois Rimle, LL.M.

2011

- Entwicklungen im schweizerischen Versicherungsrecht 2011/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2011/1
  (RVP)
- Vermeidung der Regulierung von Private Equity-Investitionen in der Schweiz (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.; Alfred Gilgen, LL.M., N.Y. BAR
- Durchsetzung von Geldforderungen nach der neuen ZPO
  Dr. Alois Rimle, LL.M.

2010

- Der Aktionärsbindungsvertrag
  Chasper Kamer, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2010/1 (Deutsch und Englisch)
  (RVP)
- Entwicklungen im Unternehmens-Daten-schutzrecht der Schweiz und der EU 1/2010
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Banken- und Kapitalmarktrecht 2010/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Versicherungsrecht 2010/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Rechtliche Rahmenbedingungen der Unternehmenssanierung
  (RVP)

2009

- Entwicklungen im schweizerischen Transaktionsrecht 2009/2 (Deutsch und Englisch)
  (RVP)
- Überstunden und Überzeit
  Dr. Franziska Buob
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/2 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/2
- Unternehmensleitung in Krisenzeiten
  Worauf es zu achten gilt
  Dr. Franziska Buob
- Entwicklungen im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2009/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im Datenschutzrecht für Unternehmen in der Schweiz und der EU 2009/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Entwicklungen im schweizerischen Transaktionsrecht 2009/1
  (RVP)

2008

- Revision des Revisionsrechtes: Eine Übersicht über die wichtigsten Neuerungen
  Sara Sager
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2008/2 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.
- Vom Prozessieren
  Dr. Franziska Buob
- Liegenschaften im Erbgang: Häufige Tücken und Fallen (Teil I: Nachlassplanung)
  Pio R. Ruoss
- Outsourcing
  Dr. Marc M. Strolz
- IP IT Outsourcing
  Pascale Gola, LL.M.
- Entwicklung im schweizerischen Versicherungs-, Banken- und Kapitalmarktrecht 2008/1 (Deutsch und Englisch)
  Dr. Alois Rimle, LL.M.

2007

- Aktuelles aus dem Bereich des Immaterialgüter- und Firmenrechts
  Dr. Martina Altenpohl
- Die „kleine Aktienrechtsreform“ und Neuerungen im Recht der GmbH
  Chasper Kamer, LL.M.
- Swiss Insurance Law Update 2007/1
  Dr. Alois Rimle, LL.M.
- Privatbestechung (Art. 4a UWG)
  Dr. Reto T. Ruoss
- Neue Phase der Freizügigkeit für EU/EFTA-Bürger, deren Familienangehörige und Erbringer von Dienstleistungen in der Schweiz
  Alfred Gilgen, LL.M.
- Revidiertes Datenschutzrecht für Unternehmen in der Schweiz
  Dr. Alois Rimle, LL.M.
- Aktuelles aus dem Bereich des Wettbewerbs- und Immaterialgüterrechts
  Chasper Kamer, LL.M.
- Actions Required under New Swiss Collective Investment Schemes Act
  Dr. Alois Rimle, LL.M.

2006

- Dokumenten- und Datenaufbewahrung im schweizerischen Unternehmen
  Dr. Alois Rimle, LL.M.
- Schweizerische Versicherungs- und Vermittleraufsicht
  Dr. Alois Rimle, LL.M.