Umsetzung des revidierten DSG

Stand: 17.07.2022

1. Worum geht's?

Das schweizerische Datenschutzgesetz (DSG) befindet sich in Revision. Die revidierte Fassung des DSG (revDSG) liegt seit längerem vor, die zugehörige Verordnung befindet sich noch in der finalen Ausarbeitung (Entwurf). Beide werden aber höchstwahrscheinlich am 1. September 2023 in Kraft treten.

Kleine Schwester der DSGVO

Das revidierte Recht ist keine Umsetzung der DSGVO, von ihr aber stark inspiriert. Es legt den Fokus auf folgende Punkte:

— **Stärkung der «Governance»**: Die Einhaltung des Datenschutzes soll dadurch gestärkt werden, dass Unternehmen bestimmte Pflichten an ihre Organisation und Dokumentation zu erfüllen haben. Das vergrössert den Aufwand der Unternehmen.

— **Stärkung der Transparenz**: Das Datenschutzrecht beruht zu einem wesentlichen Teil auf der Eigenverantwortung betroffener Personen Diese Verantwortung können sie nur wahrnehmen, wenn sie verstehen, wie mit ihren Daten umgegangen wird. Das revDSG führt deshalb eine allgemeine Informationspflicht ein: Anders als heute (mit Ausnahmen) müssen Unternehmen nach dem revDSG auch über banale Datenbearbeitung informieren. Eine Verletzung dieser Pflicht kann sogar strafbar sein.

— **Stärkung der Betroffenenrechte**: Das revDSG gibt den Betroffenen deshalb weitere Rechte, um sich über Datenbearbeitungen zusätzlich zu informieren und auf diese einzuwirken. Wichtig ist weiterhin vor allem das Auskunftsrecht, d.h. das Recht, von einem Unternehmen Angaben über der Bearbeitung der eigenen Personendaten zu erhalten. Dieses Recht kann jederzeit und aus beliebigen Gründen eingesetzt werden. Eine Falschauskunft kann strafbar sein.

— **Stärkung der Durchsetzung**: Dem EDÖB kommt bei der Durchsetzung des Datenschutzrechts eine wichtige Rolle zu (er ist zuständig, Datenbearbeitungen

bei privaten Unternehmen und bei Bundesorganen zu überwachen). Das revDSG gibt ihm erweiterte Möglichkeiten.

— **Abschreckung**: Ebenfalls der Durchsetzung dient die Abschreckung durch Strafen. Das heutige DSG sieht nur in Ausnahmefällen Bussen vor, aber nur bis CHF 10'000 und ohne praktische Vollstreckung. Nach neuem Recht können bestimmte vorsätzliche Verletzungen mit Busse bis CHF 250'000 (für die verantwortlichen Personen selbst) bestraft werden.

Zunehmender Fokus auf den Datenschutz

Der Datenschutz wird nicht nur durch die Revision des Datenschutzrechts gestärkt und verschärft. Auch die Erwartungen von Kunden, Investoren, Behörden, Partnern und des Publikums ändern sich - war der Datenschutz für Stakeholder lange Zeit kein grosses Thema, ausserhalb regulierter Branchen, gewinnt er nun stark an Beachtung.

Eine gewisse Datenschutzcompliance ist deshalb auch Teil des Managements von Stakeholdern geworden. Unternehmen können eine Auseinandersetzung mit den Datenschutz und eine angemessene Umsetzung der neuen Anforderungen deshalb nicht vermeiden.

2. Umsetzung des revidierten Rechts

Einen One-Size-Fits-All-Ansatz gibt es dabei nicht. Zu unterschiedlich sind Struktur und Komplexität der Unternehmen, Kritikalität und Umfang der von ihnen bearbeiteten Daten, Bedeutung der Datenbearbeitung für ihr Geschäftsmodell und die Erwartungen an den Umgang mit Personendaten.

Es haben sich in der Zwischenzeit aber Erfahrungswerte gebildet, die einen gewissen Best-Practice-Ansatz herausbilden. Diesen Ansatz stellen wir anschliessend im Sinne einer Hilfestellung vor allem für KMU kurz dar, mit Hinweisen zum rechtlichen Rahmen und Vorschlägen für konkrete Massnahmen. Besonders bei grossen Unternehmen und Unternehmen in einem komplexen oder regulierten Umfeld werden sich zahlreiche weitere Fragen stellen. Aber auch die längste Reise beginnt bekanntlich mit dem ersten Schritt.

Es versteht sich von selbst, dass die folgende Darstellung weder vollständig noch für alle Fälle passend ist - Unternehmen müssen sich mit dem Datenschutz beschäftigen und können dabei vieles, aber nicht alles auslagern. Entsprechend sind die folgenden Hinweise keine Rechtsberatung. Sie stehen ausserhalb eines Mandats, und wir geben keine Gewährleistung und übernehmen auch keine Haftung.

3. Handlungsempfehlungen

3.1. Planung

Die Umsetzung des revidierten Gesetzes verlangt eine gewisse Planung. Aber mit Augenmass - umfangreiche Projektplanungen haben sich jedenfalls für KMU wenig bewährt. Meist lassen sich die wesentlichen Aufgaben recht rasch festlegen. Eine detaillierte Gap-Analyse kann sinnvoll sein, eignet sich oft aber eher für einen späteren Zeitpunkt.

Wichtig ist aber, dass ein Projekt - auch ein kleines - vom Management gestützt wird. Das verlangt messbare Erfolge, und auch dies spricht dafür, die Planung nicht ausufern zu lassen.

Allerdings ist der Aufwand der Umsetzung von der Komplexität und Grösse des Unternehmens abhängig, ebenso wie von den Anforderungen und Erwartungen der Stakeholder, d.h. bspw. der Kunden und des Publikums und bei regulierten Unternehmen auch des Regulators (der FINMA, des BAG usw.). Und je heikler die bearbeiteten Daten sind und je grösser ihr Gewicht im Geschäftsmodell, desto höher sind die Risiken für das Unternehmen. Auch ein Bezug zu Europa spielt eine Rolle - u.U. müssen alle oder bestimmte Datenbearbeitungen auch der DSGVO entsprechen.

Bei Startups spielt auch ein möglicher Exit eine Rolle - hier sollte das Unternehmen bei einer Due Diligence nicht ganz durchfallen.

Schliesslich spielt ein Konzernverbund eine grosse Rolle. Ein KMU, das Teil einer Gruppe mit Auslandsbezug ist, muss u.U. die DSGVO umsetzen (wobei das selten zu 100% erforderlich oder möglich ist), kann idealerweise aber auch auf bestehende Grundlagen aus dem Konzern zurückgreifen.

Todos

- Überlegungen zu den genannten Punkten anstellen
- mit dem Management über eine Umsetzung des revidierten Datenschutzrechts sprechen
- überlegen, wer das Projekt intern leiten soll und wer dafür die Verantwortung trägt
- falls erforderlich fehlendes Fachwissen einkaufen
- Ressourcen planen, ggf. externe Anbieter um Offerten bitten

— Zeitplan abstecken

3.2. Weisungen und Policies

Das revidierte Recht traut Unternehmen nicht mehr zu, den Datenschutz zu gewährleisten, ohne dass eine gewisse Struktur und Organisation geschaffen wird. Es ist zwar noch wesentlich prinzipienorientierter als die DSGVO, aber bestimmte Abläufe und Rahmenbedingungen sind zu dokumentieren.

3.2.1. Weisung zum Datenschutz

Zunächst sollte ein Unternehmen die Grundsätze seines Umgangs mit Personendaten in einer **internen Richtlinie (Policy)** regeln. Zwingend ist das nicht, aber aus mehreren Gründen sinnvoll:

— Eine Policy legt die Organisation des Unternehmens im Bereich des Datenschutzes fest, und besonders auch die internen Zuständigen und Verantwortlichkeiten. Damit ist eine Policy auch ein Element der korrekten Delegation und damit Entlastung der Führungsorgane.

— Eine Policy hilft, das Bekenntnis des Unternehmens zu einem angemessenen Datenschutz intern zu kommunizieren.

— Es ist absehbar, dass Unternehmen durch Kunden und ggf. bei einer Übernahme öfter nach einer Policy gefragt werden.

— Wenn eine Datenschutzverletzung geschieht, hilft eine Policy bei der Verteidigung oder zumindest beim Argument, dass man den Datenschutz nicht ganz ausser Acht gelassen hat.

3.2.2. Weitere Policies und Anweisungen

Ob weitere Policies, Weisungen oder Anleitungen erforderlich sind, hängt von der Komplexität der Organisation und von seinem Geschäftsmodell ab.

Sinnvoll ist aber jedenfalls eine Policy zur **Datenlöschung**. Dazu finden sich anschliessend Hinweise.

Auch der Umgang mit **Datensicherheitsverletzungen** ist wesentlich. Zum einen führt das revDSG eine Pflicht ein, Sicherheitsverletzungen unter bestimmten Voraussetzungen dem EDÖB oder den betroffenen Personen mitzuteilen. Dafür steht nur eine beschränkte Frist zur Verfügung. Zum anderen führt ein falscher Umgang mit Sicherheitsverletzungen zu Reputationsrisiken. Unternehmen müssen sich deshalb überlegen, wie sie sicherstellen, dass Sicherheitsverletzungen rasch entdeckt und intern aufgenommen oder eskaliert werden.

Ebenfalls sinnvoll kann eine generelle **Anleitung** sein – im Sinne möglichst einfacher und konkreter Hinweise –, wie generell mit aussergewöhnlichen Situationen umzugehen ist, bspw. mit einer Sicherheitsverletzung, einem Auskunftsbegehren oder auch dem Einsatz neuer Software.

Todos

- Ausarbeitung eines Entwurfs einer Policy mit den wesentlichen Grundsätzen des Datenschutzes im Unternehmen
- Abstimmung mit den internen betroffenen Personen - wer eine Aufgabe erhält, muss sie akzeptieren und dafür entsprechend vorbereitet werden (und die erforderlichen Ressourcen haben)
- Überlegungen, ob weitere Policies oder Anweisungen sinnvoll sind, z.B. für die Datenlöschung oder den Umgang mit Sicherheitsverletzungen
- ggf. Ausarbeitung weiterer Policies oder Anweisungen

3.3. Bearbeitungsverzeichnis

Das revidierte Gesetz verlangt, dass Unternehmen ein Verzeichnis ihrer Bearbeitungstätigkeiten führen - ein Verzeichnis in Textform (sofern die revidierte Verordnung nichts anderes festlegt), z.B. als Excel, in Confluence, in einem anderen Tool oder mit einer spezialisierten Software. In diesem Verzeichnis sind für einzelne Arten von Bearbeitungen (z.B. «Bewerbermanagement», «Lohnzahlungen», «Newsletterversand» usw.) bestimmte Angaben zu erfassen.

Das gilt nicht nur für sogenannte Verantwortliche, sondern auch für Auftragsbearbeiter wie z.B. IT-Dienstleister.

Allerdings sind Unternehmen von dieser Pflicht voraussichtlich befreit, wenn sie weniger als 250 Mitarbeitende beschäftigen. Solche Unternehmen müssen sich überlegen, ob sie freiwillig ein Bearbeitungsverzeichnis führen wollen. Dafür spricht, dass es als Teil einer guten Compliance angesehen wird, was bei einem Verstoss Argumente in die Hand gibt. Dagegen spricht, dass die laufende Führung des Verzeichnisses aufwendig sein kann, und dass es dem Unternehmen praktisch gesehen oft wenig nützt, wenn es qualitativ nicht gut und in Abläufe eingebettet ist.

Todos

— Prüfung, ob die Ausnahme von der Pflicht greift, ein Bearbeitungsverzeichnis zu führen

— Bestimmung, in welcher Form ein Bearbeitungsverzeichnis geführt werden soll

— Definition einer Vorlage (das kann ein einfaches Excel mit einer Zeile pro Bearbeitungstätigkeit sein)

— Überlegungen zum Vorgehen für die initiale Erhebung und später die laufende Aktualisierung des Verzeichnisses

— ggf. Anleitung an die betreffenden Stellen (Hinweise, Beispiele für die Erfassung usw.)

— Erfassung der Bearbeitungstätigkeiten

3.4. Informationspflicht

Das heutige DSG verlangt nur in Ausnahmefällen eine ausdrückliche Information über die Bearbeitung von Personendaten (wenn besonders schützenswerte Personendaten wie z.B. Gesundheitsdaten oder Persönlichkeitsprofile beschafft werden). In den meisten Fällen reicht es, wenn sich eine Bearbeitung von selbst versteht.

Das ändert sich mit dem revidierten Gesetz. Analog zur DSGVO verlangt das Gesetz bei allen Bearbeitungen eine Information, sofern nicht eine Ausnahme greift. Das gilt sogar bei selbstverständlichen und trivialen Bearbeitungen. Damit wird zwar niemandem geholfen, aber eine Verletzung dieser Pflicht kann sogar strafbar sein.

Unternehmen sollten deshalb über ihre Bearbeitungen informieren, meist in Form von Datenschutzerklärungen. Das sind Hinweise oder Dokumente, die sich zur Datenbearbeitung äussern - sie sind nicht Vertragsbestandteil und sollten in der Regel auch nicht Teil von AGB sein.

Welche und wie viele Datenschutzerklärungen erforderlich sind, ist vom Geschäftsmodell abhängig. Meistens werden es aber etwa folgende sein:

— eine allgemeine Datenschutzerklärung, die auf der Website bereitgestellt wird und die die meisten Bearbeitungen abdeckt, z.B. den Umgang mit Endkundendaten, mit Daten von Kontaktpersonen bei Kunden und Lieferanten, beim Marketing, bei der Zusammenarbeit mit Partnern usw.;

— eine separate Cookie Notice, die den Umgang mit Personendaten über die Webseite(n) und ggf. Apps erklärt. Sie kann Teil der allgemeinen Datenschutzerklärung sein, aber eine eigene Erklärung entspricht oft mehr den Erwartungen;

— eine Datenschutzerklärung für Mitarbeitende. Sie kann sich auch zu Stellenbewerbenden äussern, sofern hier nicht eine eigene Datenschutzerklärung verwendet wird.

Eine andere Frage ist, auf welche Weise betroffene Personen (d.h. Personen, deren Daten bearbeitet werden), auf die passende Datenschutzerklärung hingewiesen werden. Dafür gibt es keine One-Size-Fits-All-Lösung - entscheidend sind die Schnittstellen mit den betroffenen Personen. Sinnvoll sind aber Hinweise

— in Verträgen, zumindest in Verträgen mit Endkunden (AGB) und in Arbeitsverträgen oder -reglementen,

— in der Fusszeile der Webseite und in Apps,

— in Korrespondenz mit betroffenen Personen, z.B. in einer E-Mail-Signatur, in Rechnungen, Bestellformularen usw. Hier können und sollten auch Bestandskunden, deren Daten vor dem Inkrafttreten des neuen Gesetzes beschafft worden sind, auf die Datenschutzerklärung aufmerksam gemacht werden.

Einwilligungen sind nach schweizerischem Datenschutzrecht dagegen nicht häufig erforderlich. An Einwilligungen ist aber zu denken, wenn besonders schützenswerte Daten (z.B. Gesundheitsdaten) weitergegeben werden und beim E-Mail-Marketing.

Todos

— Ausarbeitung der Datenschutzerklärungen - dafür stehen Muster zur Verfügung, die sich mit den notwendigen Anpassungen als Ausgangsmaterial eignen. Ein ausführliches Muster findet sich hier, und weitere Muster sind verfügbar

— Überlegungen zu Hinweisen auf die Datenschutzerklärungen bspw. in Verträgen und Musterkorrespondenz

— allenfalls Überlegungen zu Anpassungen der Datenbearbeitungen, z.B. zur Ablösung oder Einstellung bestimmter Analysetools auf Websites.

Es kann zudem sinnvoll sein, auch an andere Informationspflichten zu denken, z.B. ein Impressum bei Online-Angeboten.

3.5. Verträge

Das revidierte DSG verlangt in bestimmten Fällen den Abschluss von Verträgen. Das ergibt sich daraus, dass das DSG verschiedene Rollen von Unternehmen unterscheidet:

— **Verantwortlicher**: Das ist dasjenige Unternehmen, das Daten im eigenen Interesse bearbeitet oder bearbeiten lässt und das über diese Bearbeitung bestimmt. Ein Unternehmen ist z.B. ein Verantwortlicher für die Bearbeitung der Daten seiner Mitarbeiter und seiner (End-)Kunden.

— **Auftragsbearbeiter**: Ein Auftragsbearbeiter bearbeitet auch Daten, aber nur als Dienstleister für einen Verantwortlichen. Ein Auftragsbearbeiter ist z.B. ein Hostingdienstleister oder der Anbieter einer Cloud-basierten Softwarelösung: Hier bestimmt der Verantwortliche über die Art und Weise der Datenbearbeitung. Manche Dienstleister sind allerdings auch Verantwortliche - dann, wenn sie über die Art der Datenbearbeitung weitgehend selbst entscheiden. Ein Beispiel ist eine Anwaltskanzlei.

3.5.1. Auftragsbearbeitung

Weil sich diese Rollen bei der Bearbeitung so stark unterscheiden, tun es auch die datenschutzrechtlichen Pflichten. Der Verantwortliche muss das volle Pflichtenprogramm des DSG einhalten (deshalb heisst er auch «Verantwortlicher»). Ein Auftragsbearbeiter muss und kann das nicht im gleichen Umfang, weil er bis zu einem gewissen Grad vom Verantwortlichen gesteuert wird - er ist sozusagen dessen verlängerter Arm.

Dies verlangt aber auch, dass der Verantwortliche und der Auftragsbearbeiter ihre Beziehung vertraglich regeln. Dazu müssen sie einen sog. Auftragsbearbeitungsvertrag schliessen - Regeln bspw. über das Weisungsrecht des Verantwortlichen, sein Recht, die Datenbearbeitung zu prüfen, und die Pflicht des Auftragsbearbeiters, die Datensicherheit zu gewährleisten und beim Ende seines Auftrags Daten zu löschen.

Fehlt ein solcher Vertrag bei einer Auftragsbearbeitung, kann das nach dem revidierten DSG strafbar sein. Der Verantwortliche muss deshalb sicherstellen, dass er solche Verträge geschlossen hat oder schliesst. Bei Anbietern von Standardlösungen ist das i.d.R. der Fall - sie schliessen solche Verträge in ihre Standardverträge ein. Bei anderen Anbietern können sie aber fehlen.

Und besonders konzernintern fehlen solche Verträge nicht selten, wenn eine Gesellschaft konzernintern zentrale Dienstleistungen wie z.B. ein CRM-System betreibt. Konzernintern können auch weitere Punkte zu regeln sein, z.B. der Arbeitseinsatz von Mitarbeitenden einer Gesellschaft für eine andere.

3.5.2. Gemeinsame Verantwortung

Neben der Auftragsbearbeitung gibt es auch die gemeinsame Verantwortung, wenn mehrere Unternehmen gemeinsam über eine Bearbeitung entscheiden. Das Konzept ist reichlich unklar, aber konzernintern ist eine gemeinsame Verantwortung häufig, wenn mehrere Konzerngesellschaften dieselbe Lösung z.B. für das Mitarbeitermanagement oder ein CRM verwenden. Auch bei Partnerschaften, bei denen Daten für ein gemeinsames Produkt bearbeitet werden, sind gemeinsame Verantwortlichkeiten nicht selten. Anders als die DSGVO verlangt das revidierte Gesetz nicht ausdrücklich eigene Vereinbarung zwischen den gemeinsam Verantwortlichen. Sie ist aber sinnvoll, denn hier ist eine Abgrenzung der Zuständigkeiten und Verantwortung oft schwierig. Es sollte daher i.d.R. vereinbart werden, wer die betroffenen Personen informiert, wer sich um Auskunftsbegehren kümmert, wer die Datensicherheit gewährleistet usw.

3.5.3. Übermittlung ins Ausland

Ein wichtiges Thema ist derzeit die Übermittlung von Personendaten ins Ausland. Sie verlangt u.U. ebenfalls den Abschluss oder eine Prüfung von Verträgen. Dazu finden sich anschliessend separate Hinweise.

Todos

— Zusammenstellung der bestehenden Verträge mit Dienstleistern bzw. Kunden, wenn dabei Daten bearbeitet werden

— Prüfung der entsprechenden Rollen

— Prüfung der Verträge auf den erforderlichen datenschutzrechtlichen Mindestinhalt

— ggf. Ausarbeitung einer Standardvereinbarung für Auftragsbearbeitungen, besonders durch Unternehmen, die eine so starke Stellung haben, dass sie bei Dienstleistern ihre eigenen Verträge verwenden können, und bei Dienstleistern, die Kunden solche Verträge anbieten müssen oder wollen (besonders IT-Dienstleister)

— ggf. Abschluss entsprechender Verträge mit Lieferanten, Kunden und Partnern

3.6. Bekanntgabe von Daten ins Ausland

3.6.1. Übermittlung ins Ausland

Das Datenschutzrecht will Schutz gewährleisten. Es kann eine Übermittlung in Staaten deshalb nicht schrankenlos zulassen, wenn dort der erforderliche Schutz fehlt. Wie die DSGVO und das heutige DSG erlaubt das revidierte DSG eine solche Übermittlung deshalb zunächst nur, wenn der Empfängerstaat einen angemessenen Datenschutz gewährleistet. Werden Daten unzulässig exportiert, kann das nach dem revidierten DSG strafbar sein.

Das ist bei allen **EWR-Staaten** und wenigen weiteren Staaten der Fall (der EDÖB führt eine Liste solcher Staaten, die Länderliste). Bei Angaben über juristische Personen sind laut EDÖB allerdings auch in solchen Staaten weitere Massnahmen erforderlich (was in der Praxis weitgehend ignoriert wird).

Bei **anderen Staaten** wie z.B. den USA oder Indien ist eine Übermittlung nur zulässig, wenn der fehlende gesetzliche Schutz durch den Abschluss eines ausreichenden Vertrags mit dem Empfänger ausgeglichen wird. Das sind fast immer die sogenannten **Standardvertragsklauseln** oder «SCC», die von der EU-Kommission ausgearbeitet wurden.

Der EDÖB hat diese SCC als ausreichend akzeptiert. Allerdings verlangt er, dass sie in einigen Punkten an das schweizerische Recht angepasst werden.

Es gibt auch Ausnahmen – unter bestimmten Umständen kann auch bei solchen Staaten auf den Abschluss eines Vertrags verzichtet werden. Das sind aber eher seltene Ausnahmen, die im Rahmen der Umsetzung des revidierten DSG kaum eine Rolle spielen.

Unternehmen sollten deshalb prüfen, ob sie Daten ins Ausland bekanntgeben. Das wird sehr oft der Fall sein - nicht nur bei einer Kooperation mit Unternehmen im Ausland, sondern besonders auch bei IT-Dienstleistern. Finden sich diese Dienstleister in einem Staat, der keinen angemessenen Datenschutz gewährleistet, müssen die Verträge mit ihnen geprüft werden, ob sie die notwendigen Bestimmungen enthalten.

3.6.2. «Schrems II»

Die erwähnten SCC, die z.B. mit Datenempfängern in den USA zu schliessen sind, sind nur dies – Verträge. Anders als das lokale Recht binden sie die Behörden nicht. Haben diese zu weitgehende Zugriffsrechte auf übermittelte Daten, ist dies aus der Optik des DSG problematisch, denn diese Rechte können durch die SCC kaum beschränkt werden.

Der europäische Gerichtshof hat deshalb entschieden (im berüchtigten «Schrems II»-Urteil), dass sich ein Exporteur nicht blind auf die SCC verlassen darf. Er muss vielmehr das lokale Recht prüfen, und wenn dieses überschiessende Zugriffsrechte vermittelt, muss er weitere Massnahmen treffen.

Kaum ein Thema ist derzeit so umstritten wie dieses. Zum einen ist unklar, ob sich der Exporteur darauf verlassen darf, dass die lokalen Behörden an den von ihm übermittelten Daten kein Interesse haben werden (was in den allermeisten Fällen zutreffen wird). Zum anderen ist unklar, wie dem Risiko eines Zugriffs überhaupt begegnet werden kann, denn auch technische Massnahmen können diesen Zugriff in den meisten Fällen kaum ausschliessen.

In der Praxis schätzen Unternehmen die Risiken eines Behördenzugriffs mit einem Formular ein, und wenn die Wahrscheinlichkeit eines Zugriffs sehr niedrig ist, haben sie keinen Grund zur Annahme, dass ein Zugriff erfolgt. In diesem Fall verlassen sie sich auf die SCC. Rechtssicher ist dieses Vorgehen nicht, aber eine vernünftige Alternative fehlt.

Todos

— Bestandsaufnahme, wo Daten in Staaten übermittelt werden, die keinen angemessenen Schutz aufweisen

— Prüfung, ob auf die entsprechende Bekanntgabe verzichtet bzw. ob ein Dienstleister durch einen CH/EU-Anbieter ersetzt werden könnte

— Prüfung, ob mit dem Empfänger im entsprechenden unsicheren Staat eine Vereinbarung besteht, die die SCC einschliesst

— falls dem so ist, Prüfung, ob die SCC auf dem aktuellen Stand sind und ob sie die notwendigen Anpassungen auf die Schweiz enthalten (z.B. in Form eines standardisierten Zusatzes, eines «Swiss Addendum»)

— ggf. Abschluss weiterer Verträge (SCC)

3.7. Weitere Punkte

Neben den genannten Punkten sind natürlich weitere Punkte zu bedenken. Ohne Anspruch auf Vollständigkeit: zwei der wichtigsten Punkte sind sicher die Datenlöschung und die Datensicherheit.

3.7.1. Datenlöschung

Daten dürfen generell und schon nach dem heutigen Datenschutzrecht nicht länger aufbewahrt werden, als dafür ein legitimer Zweck besteht.

Das betrifft z.B.

— Geschäftszwecke, die eine Bearbeitung von Daten erforderlich machen, bspw. im Arbeitsverhältnis oder gegenüber Kunden und Lieferanten

— Geschäftszwecke, die nicht zwingend sind, aber legitim, z.B. die Speicherung von Daten für Marketingzwecke, zur Dokumentation, zur Erstellung von Statistiken usw.

— gesetzliche Aufbewahrungspflichten, die auch eine Aufbewahrung von Personendaten verlangen können, bspw. für Buchhaltungszwecke, im Steuerbereich und im Arbeitsverhältnis.

Wenn aber keine legitimen Gründe für eine Speicherung mehr bestehen und auch keine gesetzliche Aufbewahrungspflicht mehr gilt, müssen Personendaten gelöscht oder anonymisiert werden. Eine Löschung hat auch Vorteile - die Risiken einer Sicherheitsverletzung können sinken, die Informationspflicht wird weniger rasch verletzt und Auskunftsbegehren sind einfacher korrekt zu beantworten.

In einfacheren Verhältnissen kann diese Löschung z.T. von Hand erfolgen, bspw. bei Bewerberdossiers, bei Unterlagen von Mitarbeitern, die das Unternehmen vor langer Zeit verlassen haben oder bei ehemaligen Kunden, wenn keine Verjährungsfrist mehr greift.

Eine Löschung von Hand ist aber fehleranfällig und unvollständig. Automatisierte Löschroutinen zu implementieren kann aber eine ausgesprochen anspruchsvolle, langwierige und kostspielige Aufgabe sein, besonders bei Unternehmen, deren komplexe IT organisch gewachsen ist.

Ein vernünftiger Mittelweg - zumindest für den Beginn - ist meist eine Kombination einer Weisung zur Aufbewahrung und Löschung mit einer geeigneten Konfiguration der Applikationen. Falls sich ein System nicht so konfigurieren lässt, dass es Daten zu einer bestimmten Zeit löscht, kann eine Archivierung einen gewissen Ersatz darstellen.

Todos

— Wo mit Gewissheit veraltete Daten liegen: Beginn einer Aufräumaktion (z.B. bei geteilten Ordnern, die alte Bewerberdossiers enthalten)

— Abklärung der wesentlichen Aufbewahrungsfristen (eine Mischung aus Aufbewahrungspflichten und Verjährungsfristen), am besten in einer Lösch-Policy

— Definition von Regeln für das händische Löschen (ebenfalls in der Lösch-Policy)

— Konfiguration von Applikationen zur automatischen Löschung, soweit möglich und sinnvoll

3.7.2. Datensicherheit

Das revidierte Recht verschärft die Anforderungen an die Datensicherheit grundsätzlich nicht, sieht man von der Pflicht Meldung bestimmter Sicherheitsverletzungen ab. Nicht ausgeschlossen ist eine Strafbarkeit bei gewissen Verletzungen, aber derzeit ist das unwahrscheinlich. Was sich aber verschärft, ist die Bedrohungslage. Angriffe wie Ransom-Angriffe, CFO Frauds und andere nehmen stark zu, und sie sind oft erfolgreich.

Unternehmen müssen sich deshalb zwingend mit der Sicherheit ihrer Systeme auseinandersetzen. Das wird häufig den Einsatz externer Spezialisten verlangen. Oft können aber schon einfachere Massnahmen einen erheblichen Sicherheitsgewinn bringen, z.B. eine Prüfung, ob Zugriffsrechte noch den aktuellen Rollen und Funktionen entsprechen und Zugriffsrechte ehemaliger MItarbeitender widerrufen wurden.

Allerdings ist es damit nicht getan. Erfahrungsgemäss sind es oft Mitarbeiter, die Einfallstor einer Sicherheitsverletzung sind. Sie müssen deshalb informiert und geschult werden, z.B. um Phishing-Angriffe erkennen zu können.

Todos

— sofern die Sicherheitsmassnahmen nicht auf dem aktuellen Stand sind: entsprechende Prüfung der eigenen Systeme und Schnittstellen

— Schulung der Mitarbeitenden in einem geeigneten Mass und Turnus