Das Schweizer Datenschutzgesetz wurde revidiert und im Herbst 2020 vom Schweizer Parlament verabschiedet. Es orientiert sich an der Datenschutz-Grundverordnung der EU (DSGVO), beinhaltet aber die eine oder andere Abweichung. Die gesetzlichen Anpassungen treten voraussichtlich im Laufe des Jahres 2022 in Kraft.

Das revidierte Datenschutzgesetz (nDSG) soll mehr Transparenz über die Verwendung von Personendaten schaffen und die Mitbestimmungsrechte der Personen, deren Daten bearbeitet werden, stärken. Unter anderem ist die Kassation von Personendaten bei Wegfall der Bearbeitungstätigkeit vorgesehen, namentlich im Falle der Saldierung einer Geschäftsbeziehung.

Die Neuerungen sind beispielsweise hier (Artikel Netzwoche) detailliert beschrieben, daher seien an dieser Stelle die wichtigsten Änderungen nur kurz erwähnt:

- Stärkung der Rechte der betroffenen Personen, namentlich durch Erhöhung der Transparenz (Information über Datenbearbeitungen)
- Förderung der Prävention und der Eigenverantwortung der Datenbearbeiter
- Stärkung der Datenschutzaufsicht (durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, EDÖB)
- Ausbau der Strafbestimmungen.

Die Folgen für datenverarbeitende Unternehmen in der Schweiz sind nicht zu unterschätzen. Das nDSG betrifft die Banken als Verantwortliche ihrer (Personen-) Kundendaten ebenso wie Outsourcing-Unternehmen als Betreiber von Applikationen, welche Personendaten beinhalten. Unternehmen werden Personendaten genau(er) kategorisieren, klassifizieren und eine Inventarisierung der Systeme vornehmen müssen, damit entsprechende Massnahmen in der Datenverarbeitung umgesetzt werden können.

Die Umsetzung des nDSG verlangt folglich eine detaillierte Analyse- und Konzeptionsarbeit, bevor technische Anpassungen in den betroffenen Applikationen und allfällige organisatorische Änderungen angegangen werden können. Ja, das nDSG betrifft das ganze Unternehmen: von der Front bis ins Backoffice, Compliance und Legal, allfällige Outsourcing-Partner und als verantwortliche Organe auch die Geschäftsleitung und den Verwaltungsrat.

Wie kann die Umsetzung der neuen Anforderungen nun konkret angegangen werden?

Bearbeitungsverzeichnis

Dreh- und Angelpunkt im ersten Schritt ist das zu erstellende Bearbeitungsverzeichnis, welches die verschiedenen Bearbeitungszwecke mit den Applikationen verbindet. Dabei gilt es, zu Beginn ein gemeinsames Verständnis über personenbezogene Daten zu entwickeln - nicht alle personenbezogenen Daten müssen im Rahmen des nDSG mit der gleichen Aufmerksamkeit bedacht werden.

Das Bearbeitungsverzeichnis gibt unter anderem Auskunft über

- Den Verantwortlichen/Auftragsbearbeitenden
- Bearbeitungszweck(e)
- Rechtfertigungsgründe der Bearbeitung
- Informationspflicht des Kunden
- Herkunft der Daten
- Kategorien der betroffenen Personen und bearbeiteten Personendaten

August 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers

- Bearbeitung besonders schützenswerter Personendaten
- Aufbewahrungsdauer
- Massnahmen zur Gewährleistung der Datensicherheit
- Applikationen, in welchen die Bearbeitung stattfindet.

Erfahrungsgemäss gilt es im Bearbeitungsverzeichnis eine pragmatische Detaillierung zu erreichen: Bearbeitungen können entlang den Bank-Hauptprozessen Basis, Zahlungsverkehr, Anlegen, Finanzieren und Vorsorge erfasst werden, mit spezifischen Ergänzungen (beispielsweise Bearbeitungen im Rahmen vom Marketing-Aktivitäten).

Eine Aufstellung der Applikationen und der darin bearbeiteten Daten (kategorisiert in CID, Massen-CID und unkritisch) und Aussagen zur persistenter Datenhaltung helfen im Anschluss, die Priorisierung der anzupackenden Applikation zu erstellen.

Aus den Projekten, welche wir mit Banken umgesetzt haben, zeigt sich, dass ein phasenbasierter Ansatz sinnvoll ist: Nicht alle Personendaten können von Tag 1 an auf Knopfdruck aus den komplexen Applikationen gelöscht werden - der Aufwand für eine perfekte Umsetzung in allen Applikation ist schlicht zu gross.

Daher ist ein risikobasierter Ansatz sinnvoll. Als Beurteilungskriterium können die folgenden Grundsätze gelten: Werden in einer Applikation

- eine grosse Menge an Personendaten bearbeitet,
- sensiblere Daten (besonders schützenswerte Personendaten) bearbeitet; und/oder
- unterschiedliche und risikoreichere Datenbearbeitungen vorgenommen,

sind die Anforderungen an organisatorische und technische Massnahmen zur Gewährleistung der Datensicherheit entsprechend höher. Diese Applikationen sind also mit hoher Priorität anzugehen.

Technisches Löschungskonzept

Für die identifizierten Applikationen gilt es nun, die technische Machbarkeit der Datenkassation zu eruieren und konzipieren. Erfahrungsgemäss besteht dabei Nachholbedarf. Systeme sind eher gebaut, um Daten anzulegen, anzuzeigen und zu bearbeiten. Wie die Daten aber endgültig und kontrolliert entfernt werden können - dazu fehlt der "Löschbutton".

Somit sind die Herstellerinnen der Applikationen (mit-)gefordert: im Idealfall werden Kassationen über bewährte Prozeduren mit entsprechenden Checks and Balances durchgeführt und nicht ad hoc durch das Ausführen eines Skripts direkt auf einer Datenbank. In jedem Fall ist es wichtig, dass Abhängigkeiten zwischen den Datensätzen betrachtet werden - nicht dass durch Datenkassation "Datenleichen" entstehen.

Wichtig: auch wenn sich Banken im Sinne eines pragmatischen Ansatzes in der Regel im ersten Anwendungsfall auf die Kundensaldierung konzentrieren, ist die Löschung von gewissen Personendaten auf Kundenwunsch ebenfalls zu berücksichtigen, auch in einer laufenden Kundenbeziehung. Es wird sich allerdings zeigen, mit wie vielen solchen Kassationsbegehren die Banken in den nächsten Jahren konfrontiert werden. Unserer Erfahrung nach sind Banken bisher zurückhaltend mit der Konzeption technischer und organisatorischer Massnahmen für diese Fälle.

Umsetzung

Neben der technischen Implementierung von Kassationsfunktionalitäten und organisatorischen Anpassungen sind zwei weitere Aspekte zu betrachten:

1. Im Rahmen der Analyse zeigt sich meist, dass vor der Kassation eine Bereinigung von Personendaten in den Systemen notwendig ist. So können beispielsweise Verträge ohne "Ablaufdatum" nicht gelöscht werden. In diesem Fall ist es also wichtig, das Löschdatum zu erfassen, damit das Dokument nach der Aufbewahrungsfrist entfernt werden kann. Solche Datenbereinigungen können erfahrungsgemäss viel Aufwand generieren. Auch darum müssen die Projektaktivitäten rund ums nDSG bereits heute gestartet werden, wenn auch der Zeitpunkt des Inkrafttretens erst per Mitte 2022 realistisch ist.
2. Datenschutz und Security ist nicht (nur) Sache der IT-Abteilung, sondern Sache der Unternehmensführung. Das Bewusstsein für diese Themen muss in der Geschäftsleitung stark präsent sein. Aber: nicht nur in der Geschäftsleitung. Es bedarf einer konstanten Sensibilisierung und Schulung der Mitarbeitenden, damit das Risiko der Verletzung von Datenschutzbestimmungen minimiert werden kann. Das nDSG bietet also erneut die (notwendige) Gelegenheit, die Mitarbeitenden auf dieses wichtige Thema zu sensibilisieren.

Fazit

Die Folgen, welche das revidierte Datenschutzgesetz für Banken hat, sind nicht zu unterschätzen: neben der Dokumentationspflicht (Stichwort "Bearbeitungsverzeichnis") sind Anpassungen in Bankapplikationen, Prozessen und der Organisation zu erwarten. Entsprechend muss das Thema jetzt angegangen werden.

Bei der Swisscom beschäftigen wir uns seit Jahren mit dem Thema Datenschutz und dessen gesetzlicher Bestimmungen: sei es aufgrund unserer Swisscom-Endkunden selbst, sei es als Nummer 1-Outsourcing Partnerin im Schweizer Bankenmarkt oder sei es in der Beratung von Banken rund ums Thema Datenschutz.

Dabei hat unser Beratungs- und Compliance-Team diverse Banken begleitet: von der Interpretation des nDSG zur Konzeption bis zur Umsetzung. Auch Sie begleiten wir gerne - zögern Sie nicht, uns zu kontaktieren.

Informationen zum Autor:

Silvan Lohri
Head Consulting Swisscom Banking
Silvan.Lohri@swisscom.com
+41 79 700 47 49
LinkedIn
Website

August 2021 | Silvan Lohri, Head Consulting Swisscom Banking | Swisscom Business Customers