DSGVO: Bei den **Löschpflichten** droht das größte **Risiko**

Von Oliver Militzer

Quelle: pixabay

Datenschutz war für Banken schon immer ein wichtiges Thema. Gleichwohl bringt die Datenschutz-Grundverordnung auch für Kreditinstitute erheblichen Handlungsbedarf mit sich, weiß Oliver Militzer. So müssen Verträge, die eine Auftragsdatenverarbeitung beinhalten, neu abgeschlossen und das Spannungsfeld zwischen Compliance und Datenschutz im Blick behalten werden. Die Prozesse bei der Meldepflicht von Datenpannen gilt es klar zu regeln, für die Beauskunftung empfiehlt der Autor die Automatisierung. Die größte Herausforderung sieht er allerdings bei den Löschpflichten. Denn nicht immer ist klar, welche Aufbewahrungsfristen gelten und wann eine Aufbewahrung vertretbar ist. Red.

MiFID II, MiFIR, MAD II, MAR, EMIR, die vierte EU Geldwäscherichtlinie, aktualisierte MaRisk und MaComp – dies sind nur einige der größeren regulatorischen Neuerungen, die von Kreditinstituten allein in den letzten zwei Jahren zu implementieren waren. Doch mit der endgültigen Umsetzung von MiFID II zum 3. Januar 2018 sahen viele Experten der Branche ein Licht am Ende des Regulierungstunnels und die Chance, sich danach endlich wieder auf das Wesentliche konzentrieren zu dürfen: das überholungsbedürftige Bankgeschäft mit dem Kunden beziehungsweise das Bestehen im digitalen Wettbewerb mit altbekannten Mitbewerbern sowie neuen innovativen Fintech-Unternehmen.

25. Mai 2018 – Beginn einer neuen Zeitrechnung?

Doch wer die letzte Zeit nur auf die oben genannten Regelungen fixiert war, an dem ist vermutlich eine weitere der größten regulatorischen Neuerungen der letzten 20 Jahre vorbeigegangen – die EU-Datenschutz-Grundverordnung (DSGVO).

Juristisch gesehen, ist sie bereits seit 24. Mai 2016 in Kraft, auch wenn ihre Vorschriften erst seit dem 25. Mai 2018 anzuwenden sind. Und dennoch scheint die DSGVO für viele Unternehmen ganz überraschend zu kommen. So gab nur rund die Hälfte der verantwortlichen Manager in der deutschen Wirtschaft im Rahmen einer noch im Mai 2018 veröffentlichten Studie an, angemessen auf die DSGVO vorbereitet zu sein. Dass einige Vorstände und Geschäftsführer mit Blick auf den defizitären Stand der Umsetzung in ihrem Unternehmen in den letzten Monaten vermehrt mit Panik reagiert haben, scheint daher auch nicht besonders verwunderlich – oder doch?

Zum Autor

Oliver Militzer, KINAST Rechtsanwaltsgesellschaft mbH, Köln

Schließlich sind der Datenschutz an sich und rechtliche Verpflichtungen im Umgang mit personenbezogenen Daten nichts Neues. Vielmehr galt die deutsche, vergleichsweise strenge Umsetzung der EU-Datenschutzrichtlinie aus dem Jahr 1995 in Form des bis zum 24. Mai 2018 geltenden Bundesdatenschutzgesetzes (BDSG a. F.) sogar als Vorbild für den europäischen Gesetzgeber bei der Ausgestaltung der DSGVO. Warum also in Panik verfallen, wenn ein Unternehmen bereits nach dem BDSG alte Fassung datenschutzrechtlich gut aufgestellt war?

Datenschutz bisher nicht ganz so ernst genommen

Aus der Sicht von Kreditinstituten können hier zumindest zwei Aspekte angeführt werden.

- Zum einen führt die DSGVO tatsächlich zu einigen weitreichenden Neuerungen, die vor allem innerhalb der in der Bankenbranche anzutreffenden komplexen Unternehmensstrukturen zeit- und kostenintensive Anpassungen erforderlich machen.

- Zum anderen könnte es daran liegen, dass man es in der Vergangenheit mit dem Datenschutz vielleicht doch nicht ganz so ernst genommen hat, in Anbetracht eines

maximalen Bußgeldrisikos in Höhe von 300 000 Euro pro Verstoß. Echte Schweißperlen entstehen dagegen jedoch mit Blick auf das Sanktionsregime der DSGVO: Bis zu 20 Millionen Euro beziehungsweise 4 Prozent des weltweiten Konzernumsatzes des Vorjahres pro Verstoß werden nun fällig (Art. 83 Abs. 5 DSGVO).

Digitalisierung ist vor allem Datenanalyse

Die zunehmende Digitalisierung des Bankensektors scheint unumkehrbar. Für viele Geldhäuser geht es trotz oder gerade wegen ihrer teilweise Jahrhunderte alten Tradition um nichts Geringeres als den eigenen Fortbestand. Ein Wettlauf um die innovativsten digitalen Produkte und Dienstleistungen ist in vollem Gange.

Aus datenschutzrechtlicher Sicht bedeutet die Digitalisierung vor allem die noch differenzierte Analyse bereits vorhandener und die umfassende Gewinnung gänzlich neuer Daten als einem der wertvollsten Rohstoffe der Zukunft.

Beim Girokonto ist Datenverarbeitung zulässig

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Im Bankenbereich finden sich derartige Rechtsgrundlagen nicht selten in spezialgesetzlichen Regelungen, die den allgemeinen Normen der DSGVO grundsätzlich vorgehen (Art. 6 Abs. 1 lit. c DSGVO). So ist beispielsweise das Anfertigen einer Kopie des amtlichen Lichtbildausweises eines potenziellen Neukunden für ein Girokonto eine Verarbeitung personenbezogener Daten, die aufgrund geldwäscherechtlicher Aufzeichnungspflichten (hier: § 8 Absatz 2 Satz 2 GwG) auch datenschutzrechtlich zulässig ist.

Liegt keine spezial-gesetzliche Regelung vor, kann die Verarbeitung von Daten auch dann rechtmäßig erfolgen, wenn sie zur Durchführung eines Vertrags erforderlich ist (Art. 6 Abs. 1 lit. b DSGVO). Handelt es sich beim Girokonto eines Kunden gleichzeitig um sein Lohn- und Gehaltskonto, so verarbeitet das kontoführende Institut zwangsläufig auch Informationen darüber, bei welchem Arbeitgeber sein Kunde angestellt ist und wie hoch das monatliche Nettoeinkommen ausfällt. Die Datenverarbeitung ist hier jedoch erforderlich, um den bestehenden Girovertrag beziehungsweise den Zahlungsdiensterahmenvertrag mit dem Kunden durchzuführen.

Des Weiteren dürfen Kreditinstitute die personenbezogenen Daten ihrer Kunden verarbeiten, soweit dies zur Wahrung der berechtigten Interessen des Kreditinstituts oder eines Dritten erforderlich ist und nicht die berechtigten Interessen des Kunden im konkreten Fall überwiegen (Art. 6 Abs. 1 lit. f DSGVO). Allerdings handelt es sich bei dieser Rechtsgrundlage um einen Auffangtatbestand, der grundsätzlich eng auszulegen ist. Zudem resultiert aus einer Verarbeitung aufgrund eines berechtigten Interesses ein jederzeit ausübbares Widerspruchsrecht zugunsten des Kunden.

Anerkannte Beispiele eines berechtigten Interesses eines Kreditinstituts sind:

- Datenübermittlungen im Konzern bei Shared-Services-Organisation,
- Direktmarketing in Bezug auf ähnliche Produkte (§ 7 UWG beachten) oder
- Datenübermittlungen an Inkassobüros oder Rechtsanwaltskanzleien zur Geltendmachung beziehungsweise Verteidigung von Rechtsansprüchen.

Einwilligung der Kunden bei digitaler Neuaufstellung wichtig

Verarbeitungen von Kundendaten, die weder aufgrund einer spezial-gesetzlichen (Verpflichtungs-) Norm oder zur Durchführung des eigentlichen Vertrags noch aufgrund eines berechtigten Interesses des Kreditinstituts erforderlich sind, bedürfen grundsätzlich der Einwilligung des Kunden (Art. 6 Abs. 1 lit. a DSGVO). Im Rahmen der digitalen Neuausrichtung der Bankenbranche wird die Einwilligung des Kunden demnach eine wichtige Rolle spielen.

Dürfen Kundendaten hingegen gemäß den drei zuvor genannten Rechtsgrundlagen verarbeitet werden, so ist das Einholen einer Einwilligung vom Kunden diesbezüglich nicht nur überflüssig, sondern nicht statthaft. Eine dennoch eingeholte Einwilligung ist grundsätzlich unwirksam und kann zudem einen bußgeldbewehrten Verstoß darstellen. Insbesondere aus diesem Grund ist es für ein Kreditinstitut unerlässlich, sich über die Rechtsgrundlage jeder vorgenommenen Verarbeitung von Kundendaten im Klaren zu sein.

Verträge nicht von Zustimmung abhängig machen

Kommt hingegen nur die Einwilligung des Kunden in die Verarbeitung seiner Daten in Betracht, so muss sie unter anderem freiwillig, das heißt ohne jeglichen Zwang erfolgen (Art. 4 Nr. 11 DSGVO). Aus diesem Grund ist eine erteilte Einwilligung in der Regel dann unwirksam, wenn die Bank den Abschluss eines Vertrages oder die Erbringung einer Dienstleistung von dieser Einwilligung abhängig gemacht hat (Art. 7 Abs. 4 DSGVO).

Sicher sind den meisten Menschen die mehr oder weniger zahlreichen E-Mails in Ihrem Postfach aufgefallen, die sie unter anderem auf die aktualisierten Datenschutzinformationen hinweisen möchten. Erstaunlich, wer so alles noch Daten von einem besitzt, oder?

Auch Kreditinstitute unterliegen der Pflicht, Kunden vor der Verarbeitung ihrer personenbezogenen Daten insbesondere über den Zweck der jeweiligen Verarbeitung und die Rechtsgrundlage umfassend zu informieren (Art. 13 DSGVO). Außerdem muss darüber aufgeklärt werden, ob eine Weitergabe der Daten an Dritte erfolgt und

wenn ja, zu welchem Zweck und auf welcher Grundlage.

Über Datenweitergabe bei Auslagerungen im Konzern informieren

Als Dritte sind ebenfalls eigenständige juristische Personen im Konzern anzusehen. Entsprechend muss auch über die Weitergabe von Kundendaten im Rahmen etwaiger konzerninterner Auslagerungen beziehungsweise Service Level Agreements (SLAs) informiert werden.

Auf die aktualisierten Pflichtinformationen sollten alle Bestandskunden bereits aufmerksam gemacht worden sein. Interessenten und Neukunden sollten sie fortan im Rahmen der manuellen oder digitalen Antragsstrecke des jeweiligen Produkts zugänglich gemacht werden.

Datenverarbeitung im Auftrag: Verträge neu Abschließen

Sei es innerhalb oder außerhalb eines existierenden Konzernverbunds, Kreditinstitute bedienen sich in der Regel einer Vielzahl externer Dienstleister. Sobald Dienstleister personenbezogene Daten von Kunden oder Mitarbeitern der Auftrag gebenden Bank verarbeiten, kann es sich um eine sogenannte Datenverarbeitung im Auftrag handeln (Art. 28 DSGVO). Dies ist regelmäßig zum Beispiel bei Beauftragung eines Unternehmens zur Vernichtung von Akten und sonstigen Daten sowie bei Auslagerung der Lohn- und Gehaltsabrechnungserstellung (ohne Steuerberatung) der Fall. Aber auch die IT-Fernwartung ist regelmäßig als Datenverarbeitung im Auftrag anzusehen.

Liegt eine Datenverarbeitung im Auftrag vor, muss ein spezieller Vertrag zusätzlich zum Hauptleistungsvertrag mit dem Dienstleister geschlossen werden. Ohne Abschluss eines solchen Vertrags erfolgt die Datenverarbeitung durch den Dienstleister unter Umständen ohne Rechtsgrundlage und damit rechtswidrig. Auch etwaige bereits nach Bundesdatenschutzgesetz (alte Fassung) abgeschlossene Auftragsdatenverarbeitungsverträge haben mit der DSGVO ihre Legitimationswirkung verloren und sind daher neu abzuschließen.

Spannungsverhältnis zwischen Compliance und Datenschutz

Spätestens seit der jüngsten Finanzkrise hat die innerbetriebliche Compliance-Funktion innerhalb der Finanzindustrie in nie dagewesenem Maße an Bedeutung hinzugewonnen. Einer effektiven Compliance-Organisation geht es vor allem darum, durch regelmäßige sowie anlassbezogene Kontrollen das Unternehmen vor Vermögensschäden durch rechtswidriges Verhalten seiner Mitarbeiter beziehungsweise Kunden zu schützen. Dabei ist die Compliance-Abteilung naturgemäß daran interessiert, über möglichst weitreichende Zugangs-, Einsichts- und Auskunftsrechte zu verfügen.

Insofern existiert ein teilweise starkes Spannungsverhältnis zwischen der Sicherstellung einer effizienten Compliance-Funktion auf der einen und der Einhaltung der neuen datenschutzrechtlichen Vorgaben auf der anderen Seite. So muss für jedes Handeln der Compliance-Abteilung auf Kundenseite eine dokumentierte Rechtsgrundlage existieren. Ein pauschaler Verweis auf die Vorgaben der MaRisk, der MaComp oder des GwG erscheint dabei nicht ausreichend. Dies gilt umso mehr in Bezug auf die eigenen Mitarbeiter. Denn zur Aufdeckung von Straftaten ist eine Verarbeitung personenbezogener Daten von Beschäftigten nur dann zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat (§ 26 Abs. 1 S. 2 BDSG). Darüber hinaus muss die Verarbeitung zur Aufdeckung erforderlich und unter anderem insgesamt verhältnismäßig sein.

Da es sich im Compliance-Bereich regelmäßig um Verarbeitungsvorgänge handelt, die für den Betroffenen ebenfalls ein potenziell hohes Risiko in sich bergen, sollte der betriebliche Datenschutzbeauftragte stets proaktiv eingebunden werden.

Die Herausforderung für Banken wird in diesem Bereich künftig also mehr denn je darin bestehen, weder gegen Compliance-Verpflichtungen noch gegen Datenschutzbestimmungen zu verstoßen.

Interne Abläufe für die Meldepflicht bei Datenpannen regeln

Ebenfalls besondere Aufmerksamkeit sollten Kreditinstitute den neuen Regelungen zum Umgang mit sogenannten Datenpannen widmen. Fortan unterliegen grundsätzlich sämtliche Datenpannen einer Meldepflicht gegenüber der zuständigen Aufsichtsbehörde, ohne Rücksicht auf die Kategorie der betroffenen Daten (Art. 33 f. DSGVO). Zudem hat die Meldung innerhalb von 72 Stunden nach Bekanntwerden zu erfolgen. Dabei können zum Beispiel das Versenden eines Briefs oder einer E-Mail an den falschen Empfänger bereits meldepflichtige Datenpannen darstellen, die auch in Kreditinstituten erfahrungsgemäß relativ häufig vorkommen.

Ohne Zweifel besteht beim Umgang mit Datenpannen ein umfangreicher Handlungsbedarf. Es bedarf geregelter interner Abläufe, die sicherstellen, dass die Bank ihrer Meldepflicht form- und fristgerecht nachkommen kann und dass der die Datenpanne verursachende Umstand nachhaltig beseitigt wird.

Beauskunftungsprozesse automatisieren

Die DSGVO räumt den von einer Datenverarbeitung betroffenen Person umfangreiche Rechte ein. Der Betroffene hat das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO), Datenübertragbarkeit (Art. 20 DSGVO) und Widerspruch (Art. 21 DSGVO).

Das Auskunftsrecht (Art. 15 DSGVO) gewährt zum Beispiel Kunden und Mitarbeitern das Recht, zunächst zu erfahren, ob personenbezogene Daten von ihnen überhaupt verarbeitet werden. Wenn ja, sind im Grundsatz sämtliche Daten zu beauskunften, die in irgendeinem Zusammenhang mit der betroffenen Person stehen und von der Bank verarbeitet werden. Auch historische Daten sind umfasst.

Zu berücksichtigen sind zum Beispiel gestellte Kreditanfragen, geführte Kommunikation (Telefon, Brief, E-Mail), eingereichte Unterlagen, ehemalige Anschriften, durchgeführte Compliance-Screenings und Kreditscorings. Gleichzeitig muss über die jeweiligen Zwecke der Verarbeitung und über etwaige Empfänger der Daten Auskunft erteilt werden. Die Auskunft hat grundsätzlich innerhalb von vier Wochen und kostenlos zu erfolgen. In Anbetracht potenziell sehr umfangreicher Datensätze sind vor allem Kreditinstitute ab einer gewissen Größe gut beraten, den Prozess der Beauskunftung zu automatisieren.

Anpassungsbedarf bei der Datenübertragbarkeit

Ähnliches dürfte im Grundsatz für das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) gelten. Denn fortan hat jeder Kunde das Recht, sämtliche Daten, die er seiner Bank im Laufe einer Geschäftsbeziehung bereitgestellt hat, in einem gängigen Dateiformat zu erhalten. Auch kann ein Kunde von seiner Bank verlangen, seine Daten direkt an ein anderes Kreditinstitut zu übertragen.

Viele mögen jetzt an die seit September 2016 gesetzlich verankerte Kontenwechselhilfe (§§ 20 f. ZKG) denken, die Banken dazu verpflichtet, ihren Kunden bei einem beabsichtigten Kontenwechsel zu einem anderen Kreditinstitut durch Übertragung bestimmter Daten zu unterstützen. Allerdings ist das Recht auf Datenübertragbarkeit deutlich umfassender ausgestaltet, so dass auch hier ein gewisser Anpassungsbedarf anzutreffen sein wird.

Unklarheiten bei den Löschpflichten

Wichtiger denn je wird für Banken künftig das Löschen personenbezogener Daten sein. Gleichzeitig handelt es sich dabei aus rechtlicher Sicht und IT-seitig wahrscheinlich um eine der größten Herausforderungen, der sich Kreditinstitute europaweit derzeit ausgesetzt sehen. Doch warum ist das so? Wie eingangs bereits aufgezeigt, existiert in Europa kaum eine Branche, die so stark und komplex reguliert ist wie die Bankbranche. Neben zahlreichen bank- und kapitalmarktrechtlichen Normen sind handels-, gesellschafts- und steuerrechtliche Vorschriften sowie Arbeits- und Sozialgesetze einzuhalten. Die meisten dieser Gesetze sehen unter anderem diverse Aufbewahrungspflichten vor.

Aufgrund der oftmals vorhandenen Unklarheit darüber, welche Daten konkret für welchen Zeitraum aufbewahrt werden müssen, haben viele Geldhäuser in der Vergangenheit einen auf den ersten Blick plausiblen Ansatz gewählt: Vorhandene Daten wurden vorsichtshalber einfach gar nicht oder erst nach sehr langer Zeit, zum Beispiel nach 30 Jahren, gelöscht. Tatsächlich aber sind personenbezogene Daten unverzüglich zu löschen, wenn kein Recht mehr zur Speicherung besteht (Art. 5 Abs. 1 lit. e DSGVO).

In Bezug auf Kunden- und Arbeitnehmerdaten ist dies regelmäßig dann der Fall, wenn keinerlei vertragliche Beziehung mehr zum Betroffenen besteht zum Beispiel, weil das Konto bereits geschlossen ist oder das Arbeitsverhältnis beendet wurde und etwaige gesetzliche Aufbewahrungsfristen bereits abgelaufen sind. Zunächst ist demnach die Beantwortung der Frage relevant, ob für ein Datum überhaupt eine gesetzliche Aufbewahrungsfrist existiert beziehungsweise welchen Zeitraum diese beträgt.

Ist keine gesetzliche Aufbewahrungsfrist einschlägig, kann ein Vorhalten der Daten zur etwaigen Geltendmachung beziehungsweise Abwehr von zum Beispiel zivilrechtlichen Ansprüchen gerechtfertigt sein. In diesem Fall kann eine Zugrundelegung der in Betracht kommenden Verjährungsfristen zielführend sein.

Die aus dieser eingehenden Analyse resultierenden Ergebnisse sind in Form eines differenzierten Löschkonzepts zu dokumentieren und IT-seitig zu implementieren, sodass eine datenschutzkonforme Speicherung beziehungsweise Löschung sichergestellt ist. Das Thema „Löschkonzept" sollte von Kreditinstituten mit höchster Priorität behandelt werden. Denn dem Betroffenen im Rahmen einer Auskunftserteilung Daten beauskunften zu müssen, die eigentlich gar nicht mehr gespeichert sein dürften und damit ein schwerwiegendes, unternehmensweites datenschutzrechtswidriges Verhalten zu offenbaren, würde sicher für jede Bank den Supergau bedeuten.

Als Fazit lässt sich festhalten: Mit Inkrafttreten der DSGVO und des neuen BDSG besteht auch für Kreditinstitute grundsätzlich kein Grund zur Panik.

Gesetzliche Neuerungen als Chance begreifen

Das bedeutet allerdings nicht, dass Banken die Umsetzung und Einhaltung der neuen datenschutzrechtlichen Vorgaben nachrangig oder sogar vernachlässigend betreiben sollten. Dies gilt vor allem für Unternehmen, in denen die bereits vor der DSGVO geltende Rechtslage nicht vollumfänglich implementiert war.

Vor diesem Hintergrund ist die Branche gut beraten, die gesetzlichen Neuerungen auch als Chance zu begreifen – nämlich als Chance, den Datenschutz von Grund auf neu zu definieren und sich als Bank auf diese Weise als verantwortungsvolles Unternehmen im stetig zunehmenden Wettbewerb zu profilieren.