Unerkannte Risiken im Datenbestand

In den Ablagen und Archiven der Geldhäuser schlummern personenbezogene Informationen, deren Nutzungsfristen abgelaufen sind. Um der Datenschutz-Grundverordnung gerecht zu werden, ist systematisches Aufräumen geboten.

Olaf Pulwey

Fünf Jahre nach Einführung der Datenschutz-Grundverordnung (DSGVO) sehen sich die meisten Unternehmen aus der Finanzindustrie bestens gegen Datenschutzverstöße gewappnet. Die oft mit erheblichem Aufwand implementierten Maßnahmen und Lösungen zeigen Wirkung. Dennoch schlummern im Kundendatenbestand beinahe jedes Kreditinstituts Tausende jederzeit abmahnfähige, oft systematische Verstöße gegen die DSGVO. In vielen Banken und Sparkassen besitzen zwischen zehn und 30 Prozent der Datensätze keine Löschvormerkung, obwohl dies erforderlich wäre. Und zwischen 50 und 90 Prozent der zur Löschung vorgemerkten Datensätze verfügen über ein falsches Löschdatum und werden damit Jahre zu spät aus dem Datenbestand entfernt. Auch Dateien wie Anschreiben oder Personenlisten enthalten personenbezogene Daten. Hier entfällt im Arbeitsalltag viel zu oft die erforderliche Löschung nach der Zweckerfüllung.

Aufräumen mit Hindernissen

Laut DSGVO dürfen Kreditinstitute Kundendaten nur so lange speichern und verarbeiten, wie es für die Durchführung des Zwecks der Datenerhebung erforderlich ist. Sind die Aufbewahrungsfristen abgelaufen, gilt es, die Daten unverzüglich zu löschen. Fast alle Banken und Sparkassen haben sich unter erheblichen Investitionen in smarte Tools und Lösungen auf diese Anforderung vorbereitet, drohen doch bei Verstößen empfindliche Strafen. Trotzdem enthalten die Datenbestände weiterhin zahlreiche abmahnfähige Datenschutzverstöße. Ein Grund dafür sind so genannte löschverhindernde Merkmale, die eigentlich die irrtümliche Löschung von Datensätzen verhindern sollen. Um notwendige Maßnahmen einzuleiten, sind eine ganzheitliche Betrachtung der Sachlage sowie die zielführende Administration des Kernbankverfahrens notwendig. Das Ziel muss die Analyse eines jeden einzelnen löschverhindernden Merkmals sein. Aufgrund fehlender Übersicht und in Anbetracht der Datenflut ist dies eine schier unlösbare Aufgabe. Ein weiterer Grund sind die zur Löschung vorgemerkten Datensätze. Das System errechnet die Fristen erst ab dem Tag der Löschkennzeichnung. Somit erfolgt in vielen Fällen die Löschung nicht fristgerecht. Hunderte Projekte zeigen, dass im Ergebnis bis zu 90 Prozent der Daten länger als erlaubt im Bestand verbleiben.

Die Lösung schrittweise angehen

Ohne softwarebasierte Unterstützung ist eine vollständige Lösung des Problems kaum zu erzielen. Der Grund liegt in schwer durchschaubaren, wechselseitigen Abhängigkeiten im Kernbankverfahren und deren institutsindividueller Administration. Die verfügbare Dokumentation ist umfangreich und auf verschiedene Fachgebiete verteilt. Gezielte Lö-

Kompakt

- Im Kundendatenbestand nahezu jedes Kreditinstituts schlummern jederzeit abmahnfähige Verstöße gegen die DSGVO.
- Ursächlich hierfür können löschverhindernde Merkmale, falsche Löschdaten, aber auch vergessene Office-Dokumente sein.
- Es ist ratsam, sich schnellstmöglich einen umfassenden Überblick über die aktuellen Datenbestände zu verschaffen und Folgemaßnahmen einzuleiten.

Löschverhindernde Eigenschaften bei einer mittelgroßen Sparkasse

Art	Anzahl
Generisches Konstrukt	2.746
Rolle	11.656
Personenvertrag	6.587
Info	2.096
Freistellungsaufträge (FSA)	614
Vorgang	4.471
Sicherheit	750
Verbund	43.290
Sonstiges	886

Quelle: Foconis

sungsprojekte ermöglichen den Kreditinstituten unter anderem einen Überblick über die Anzahl der Datensätze ohne erforderliche Löschvormerkung oder mit falschem Löschdatum. Dafür bedarf es eines mehrstufigen Vorgehens.

- **Schritt 1, Ermittlung des Status quo:** Zunächst sollten die Verantwortlichen im Institut Transparenz herstellen und die Mitarbeitenden für die bevorstehende Aufgabe sensibilisieren. Software-Lösungen ermitteln jene Datensätze, denen noch keine Löschvormerkung anhängt, obwohl dies datenschutzrechtlich geboten wäre. Zugleich ist die Menge der Datensätze im aktuellen Bestand zu bestimmen, die ein falsches Historisierungsdatum aufweisen.
- **Schritt 2, Vereinbarung des Projektplans:** Es folgt der Maßnahmenauftakt rund um Datensätze, für die es geboten ist, sie mit einem Löschkennzeichen zu versehen.
- **Schritt 3, maschinelle Bereinigung:** Eine Software bearbeitet alle Datensätze, für die eine maschinelle Bereinigung möglich ist, etwa von Verbünden, per Massendatenänderung.
- **Schritt 4, zentrale Administration:** Die Projektverantwortlichen widmen sich den identifizierten Datensätzen, die durch zentrale Administration im Kernbankverfahren eine Löschvormerkung erhalten können, und nehmen zentrale Einstellungen vor.
- **Schritt 5, manuelle Bearbeitung:** Die Verantwortlichen bearbeiten manuell die kleine Restmenge, die nicht in Schritt 3 oder 4 erfasst wurde.
- **Schritt 6, Datumskorrektur:** Nun sind die Löschvormerkungen aller Datensätze auf ein korrektes Löschdatum zu prüfen. Dabei findet ein automatischer Abgleich mit den historischen Informationen statt. Das korrekte Datum sowie eine Datei für die Korrektur des Datums, das beispielsweise das Ende der Kundenvertragsbeziehung bestimmt, werden ermittelt.

Nach Abschluss aller Maßnahmen erfolgt der Vergleich der quantitativen Ziele mit den konkreten Ergebnissen. Die Verantwortlichen können nun Maßnahmen für eine dauerhafte Sicherstellung der datenschutzrechtlichen Anforderungen festlegen.

Dateien und Formulare prüfen

Ist die Herausforderung der löschverhindernden Merkmale gemeistert, folgt die Statusanalyse bei Office-Dokumenten und Formularen. Dateien wie Anschreiben, die personenbezogene Daten enthalten, bleiben im Tagesgeschäft häufig unerlaubt bestehen, obwohl sie längst ihren Zweck erfüllt haben. Für die Umsetzung sollten die Verantwortlichen zunächst ein Projekt zur initialen Bereinigung der lokalen Laufwerke und Server aufsetzen. Im Anschluss erfolgt die systematische Überprüfung der Dateibestände in regelmäßigen Abständen. Software-Lösungen untersuchen Formulardaten und Dateien, die auf lokalen Fileservern im Kreditinstitut abgelegt sind. Zunächst identifiziert das Tool Dateikopien inhaltsbasiert und somit unabhängig vom Dateinamen. Auf diese Weise lässt sich teurer Speicherplatz einsparen, der schnell Kosten in Höhe von Hunderten oder Tausenden Euro im Monat verursachen kann. Dann findet eine Prüfung auf sensible Informationen statt, deren Speicherung nicht zulässig ist. Hierzu analysiert die Software mithilfe festgelegter, so genannter Wörterbücher die Textinhalte. Es ist möglich, diese Wörterbücher bedarfsweise um spezifische, auch regionale Besonderheiten zu ergänzen und zu bewerten. Es empfiehlt sich, dieses Vorgehen innerhalb eines Pilotprojektes, zum Beispiel in einer Abteilung, zu starten und dann die Prüfung auf weitere Ordner und Verzeichnisse auszuweiten. Es folgt die Überführung in einen wiederkehrenden, automatisierten Regelprozess über alle relevanten Bereiche hinweg.

Viele ausgefeilte Maßnahmen zur Erfüllung der DSGVO bilden keinen vollständigen Schutz vor abmahnfähigen Bedrohungen. Je mehr Zeit Banken und Sparkassen bei der Bereinigung ihrer Datensätze verstreichen lassen, desto größer wird das Risiko einer Abmahnung. Ratsam ist es, sich schnellstmöglich einen umfassenden Überblick über die aktuelle Datenlage zu verschaffen, um systematisch Maßnahmen einzuleiten. ■


© Foconis

Autor
Olaf Pulwey
ist Chief Executive Officer (CEO) von Foconis.