ifb mailing

06 | 2020

Die sehr spezifische Integration Ihrer SAP Core Banking Anwendungen in eine komplexe Systemlandschaft erfordert eine maßvolle und angepasste Lösung, die fachlich korrekt die DSGVO-konforme Löschung unterstützt und technisch robust ist.

– Armin W. Sauer, Partner ifb –

ifb DSGVO FRAMEWORK
Gegen die Zerstörung des SAP Core Banking

Die europäische Datenschutzgrundverordnung, kurz DSGVO, regelt seit 2018 EU-weit die Verarbeitung personenbezogener Daten. Auch für Banken gilt damit: Persönliche Kundendaten müssen proaktiv gelöscht werden, sobald der Zweck der Datenerhebung erlischt. Bei Verstößen gegen das Recht auf Löschung drohen Strafen von bis zu 4 Prozent des Vorjahresumsatzes. [1]Die geforderte DSGVO-Konformität bereitet IT- und Compliance-Abteilungen jedoch größtes Kopfzerbrechen, denn die Daten werden oft in verschiedenen SAP-Modulen verarbeitet. Ohne Berücksichtigung ihrer Interdependenzen gefährdet die isolierte Löschung die Integrität des SAP Core Banking Systems massiv. Mit unserem Framework gehen wir einen neuen Weg. Wir setzen auf Anonymisierung der Daten und sichern damit zugleich Ihre DSGVO-Konformität und die Funktionsfähigkeit des SAP Core Banking Systems.

Die Ermittlung der Zweckbindung von Daten in IT-Anwendungen

Ist eine Vertragsbeziehung wie beispielsweise ein Darlehensvertrag mit einer natürlichen Person beendet und die gesetzliche Aufbewahrungspflicht erfüllt, müssen die personenbezogenen Daten der Betroffenen laut DSGVO aus IT-Anwendungen und Archiven proaktiv durch die Bank gelöscht werden. Die IT-Anwendungen in der Regel unterstützen diese DSGVO-konforme Löschung nicht standardmäßig. Da die Kundendaten häufig in verschiedenen Anwendungen liegen, muss ihre Zweckbindung durch umfangreiche Analysen bestimmt werden.

Die Begriffe „Datenkategorie“ oder „Datenart DIN66398“ beschreiben die Zweckbindung personenbezogener Daten laut DSGVO und damit eine Gruppe von Daten, die für einen Zweck wie z.B. einen Darlehensvertrag erfasst, verarbeitet und gespeichert werden. So können die aktiven Verarbeitungszeiten und gesetzlichen Aufbewahrungsfristen für diese Datenart sowie der Zeitpunkt ihrer Löschung definiert werden. In der Praxis wird die Zweckbindung der Daten prozessorientiert bestimmt, indem die datenverarbeitenden

Unser DSGVO-Framework ist ein erprobter Leitfaden zur DSGVO-konformen Umrüstung Ihres SAP Core Banking Systems.

Basis unseres DSGVO-Frameworks ist unsere weit reichende Erfahrung mit SAP Core Banking-Projekten.

Das ifb-Framework bietet Ihnen einen stringenten Fahrplan für die Konzeption und Umsetzung effektiver Löschstrategien, um personenbezogene Daten aus dem SAP Core Banking System zu entfernen. Dabei passen wir das Vorgehen optimal auf ihre individuellen Anforderungen an.

Wir beraten Sie und zeigen auf, wie Sie Ihre Ziele bestmöglich erreichen. Wir wünschen viel Spaß beim Lesen!

Ihr ifb Team

[1] Siehe Europäische Union (EU): Verordnung 2016/679 (Datenschutz-Grundverordnung), Art. 83 Abs. 5 (2018); Landesbeauftragter für Datenschutz und die Informationssicherheit Rheinland-Pfalz: „EU-Datenschutzgrundverordnung“, unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/Broschuere_DS-GVO_2-2018.pdf (abgerufen am 30.06.2020)

Prozesse bestimmt werden. Wir erweitern dieses Vorgehen. Über die datenverarbeitenden Prozesse werden die beteiligten IT-Anwendungen ermittelt. Beim Darlehen sind dies beispielsweise die SAP Core Banking Anwendungen SAP-GP, SAP-CML, SAP-CMS und SAP-BCA. Das Vorgehen ermöglicht dann eine detaillierte Analyse der Verwendungszwecke der Daten in diesen SAP-Modulen und die Konkretisierung ihrer Zweckbindung im Gesamtsystem. Auch die fachlichen und technischen Abhängigkeiten in der IT-Architektur werden berücksichtigt.

Das technische Löschen bedroht die Integrität des SAP Core Banking Systems

Die anwendungsorientierte Betrachtung der Datenarten legt die Implementierung von organisatorischen und technischen Löschmechanismen in den IT-Anwendungen nahe. Doch dies ist leichter gesagt als getan und führt leicht in eine Sackgasse. Die verschiedenen SAP Core Banking Anwendungen stehen aufgrund ihrer hohen Integration in komplexen Abhängigkeiten zueinander. Abbildung 1 zeigt, dass die Geschäftspartner in der Anwendung SAP-GP Beziehungen zueinander haben, die auf einem Darlehensvertrag (SAP-CML) und einer Sicherheit (SAP-CMS) beruhen. Daher reicht allein die Betrachtung der Beendigung des Darlehensvertrages nicht für die Löschentscheidung aus, während weitere direkte oder indirekte Vertragsbeziehungen noch bestehen.

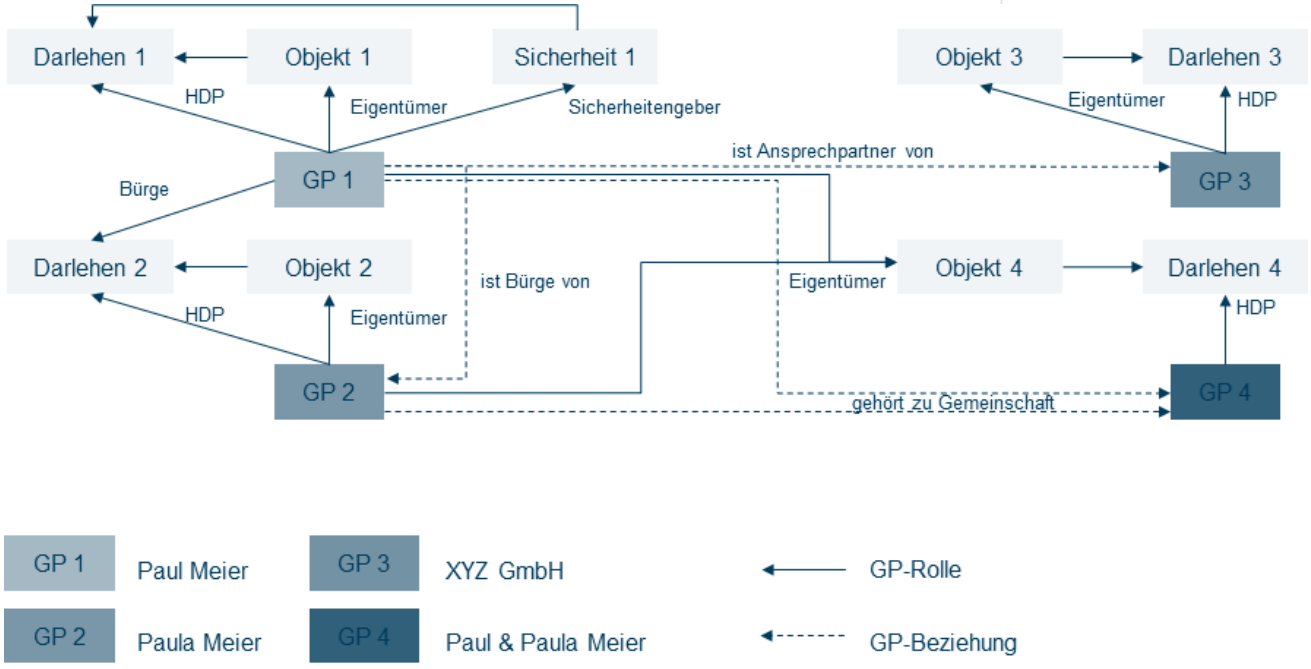

Abb. 1: Geschäftspartnerbeziehungen im SAP Core Banking

Die isolierte Betrachtung einer Anwendung wie z.B. SAP CML zur Festlegung technischer Löschmechanismen für personenbezogene Daten birgt aufgrund der engen Verknüpfung mit anderen SAP Core Banking-Modulen unwägbare Auswirkungen auf die Funktionsfähigkeit des gesamten SAP-Systems: Zur Löschung von Datensätzen im SAP Core Banking müssen die zu löschenden Datenobjekte wie z.B. Geschäftspartner und Darlehensvertrag als zusammenhängende Einheit betrachtet werden. Darlehensverträge mit unterschiedlich langer Zweckbindung können dann nur nach Beendigung der Gesamtgeschäftsbeziehung mit dem zugehörigen Geschäftspartner gelöscht werden. Die isolierte Löschung des Darlehensvertrages nach Verfall der Zweckbindung würde sonst die Integrität des SAP

Core Banking zerstören. So stößt die vollständige Umsetzung der DSGVO-Konformität in der Praxis hier an ihre Grenzen.

Unser Ansatz: Anonymisieren statt Löschen

Unser DSGVO-Framework setzt auf einen alternativen Lösungsweg: Die Anonymisierung der Daten. Damit umschiffen wir die skizzierten Probleme und reduzieren Aufwand und Komplexität der DSGVO-Projekte. Durch die Anonymisierung wird die Anwendung der DSGVO unnötig, da keine Rückschlüsse auf die natürliche Person mehr möglich sind. Im Vergleich zum Löschen der Daten in SAP Core Banking-Anwendungen liegt ein wesentlicher Vorteil der Anonymisierung im Erhalt der technischen Schlüssel zur Verknüpfung der Datenbanktabellen. Dies begünstigt die Entfernung von Datenarten mit unterschiedlichen Löschfristen, die über eine technische Verknüpfung verfügen. Und noch eine weitere Herausforderung deckt unser Framework ab: Neben ihrer Systemabhängigkeit sind SAP Core Banking-Anwendungen durch Eigenimplementierungen und Softwareerweiterungen von Drittanbietern in der Regel stark individualisiert. Personenbezogene Daten aus den Anwendungen zu entfernen erfordert umfangreiche Analysen der Datenstrukturen, um Datenbankfelder zu ermitteln, die personenbezogene Daten enthalten und diese aus der Datenbank zu entfernen. Um den Aufwand für die Identifizierung und Anonymisierung zu reduzieren, anonymisieren wir unter Berücksichtigung externer Systemabhängigkeiten einen gesamten Datensatz anstelle einzelner Felder.

Das ifb-DSGVO-Framework: Ein systematisches Phasenmodell für Ihre Ziele

Die individuelle Implementierung Ihrer SAP Core Banking Anwendungen erfordert eine individuelle Lösung angepasst auf Ihre Systemanforderungen. Basierend auf der SAP Core Banking Expertise unseres Hauses und in Zusammenarbeit mit DSGVO Experten haben wir einen Leitpfaden zur DSGVO-konformen Entfernung von personenbezogenen Daten aus Ihren SAP Core Banking Anwendungen entwickelt.

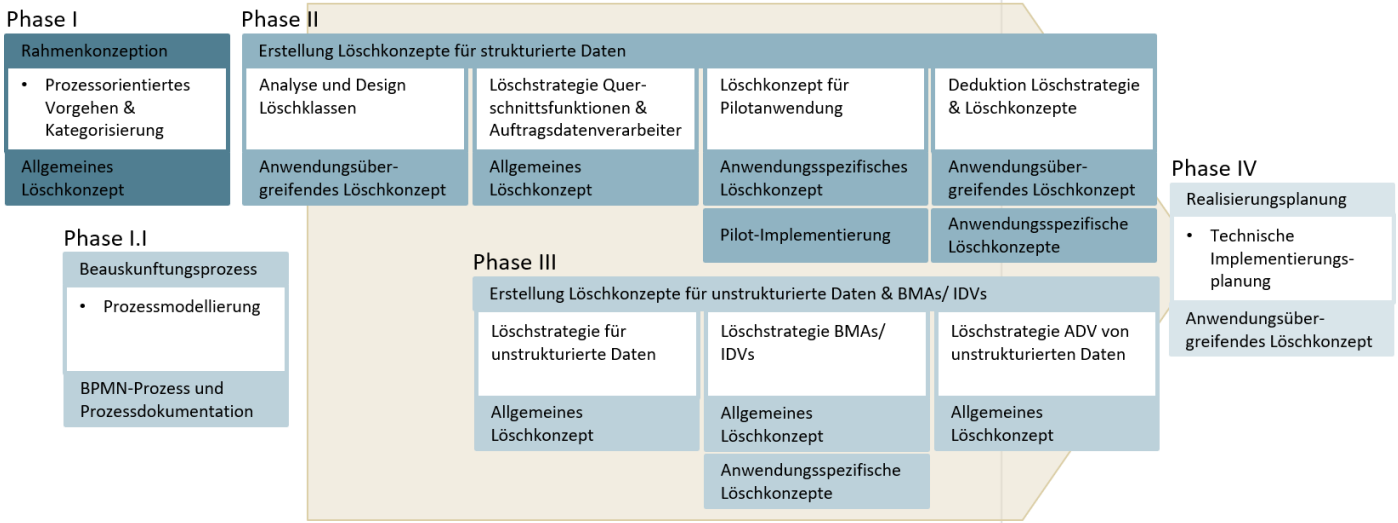

Abb. 2: Schematische Darstellung des ifb DSGVO-Frameworks

Sie möchten Näheres über das ifb DSGVO-Framework erfahren?

Nehmen Sie einfach Kontakt mit uns auf! Gerne vereinbaren wir einen Termin mit Ihnen – auch für ein Web-Meeting. Haben Sie Anmerkungen und Feedback? Wir stehen gerne Rede und Antwort.

ANSPRECHPARTNER:

Armin W. Sauer
Partner
armin.sauer@ifb-group.com

Mirko Rohde
Director
mirko.rohde@ifb-group.com

Würden Sie gerne weitere Informationen zum ifb DSGVO Framework erhalten?

Oder möchten Sie einen Termin mit uns vereinbaren?

Wir freuen uns auf Ihre E-Mail:
info@ifb-group.com

Oder rufen Sie einfach an:
+49 (0)221 921841-0