Christoph Wildensee

Yvonne Wick

SAP®-Sicherheit

Die Abrechnung des Aufsichtsratsmandats im SAP Core – Eine mögliche datenschutzrechtliche Problematik

Einleitung

Unternehmen machen es sich häufig einfach, wenn es um die IT-Abbildung betriebswirtschaftlicher Prozesse geht. Nicht immer wird dabei die Variante gewählt, die sowohl den Prozess adäquat abbildet als auch die hierauf wirkenden Compliance-Bedingungen umfassend erfüllt. Der Fall, der hier dargeboten wird, ist datentechnisch zwar unspektakulär, erscheint datenschutzrechtlich jedoch mehr als bedenklich. Die Mitglieder des Aufsichtsrates werden im SAP Core als Lieferanten abgebildet, um darüber die Abwicklung der Zahlungsströme zu gewährleisten. Und dies erfolgt berechtigungsundifferenziert.

Aufsichtsratsmitglieder erhalten für ihre Tätigkeit Aufwandsentschädigungen (Ausschussteilnahmen, Sitzungsgeld etc.), die das Unternehmen an sie zahlt. Das SAP Core bietet sich hier methodisch durchaus an, da die Mitglieder analog zu einem Berater über den Lieferantenstamm und den ordentlichen Zahlungsausgleichsmechanismus/Zahllauf des SAP-Systems behandelt werden können und dies SAP-technisch eine unkomplizierte Angelegenheit ist. Lieferanten werden z.B. über die Transaktion „Kreditoren anlegen“ (FK01) hinzugefügt. Eine Abbildung als Lieferant mit Hinterlegung der Adresse und Bankverbindung ist die Folge (Tabellen LFA1, LFB1, LFC1, LFBK, auch BSAK). Im Feld „Kontengruppe Kreditor“ (LFA1-KTOKK) kann eine separierte Kontengruppe zugewiesen werden.

Sofern aber dieser separierende Aspekt nicht beachtet, sondern eine Gruppe gewählt wird, die eine Vermengung dieser Inhalte mit einer Vielzahl weiterer Vorgangsarten bedeutet, können die Zahlungsinformationen zu den einzelnen Mitgliedern nicht mehr wie angedacht im kleinen Kreis gehalten werden. In unserem Fall erfolgte die Zuweisung zur Gruppe „Sonstige Verbindlichkeiten" (KTOKK=**SONS**) und dem Abstimmkonto „Verschiedene andere Verbindlichkeiten".

Auch auf eine weitere Vorgehensalternative soll an dieser Stelle kurz eingegangen werden: Die Abbildung der Zahlungen über ein Kreditoren-CpD-Konto, das als Sammler dient. CpD-Konten (Conto-pro-Diverse) enthalten im Stammsatz keine lieferantenspezifischen Informationen, denn das Konto wird für mehrere Lieferanten genutzt. Vielmehr werden die spezifischen Angaben wie etwa Anschrift und Bankverbindung während der Buchungsbelegerfassung eingegeben. Wesentlich sind also die Tabellen BKPF und BSEG (Buchhaltungsbelegkopf und -segment), BSEC (als CpD-Belegsegment) mit REGUH (Regulierungsdaten aus Zahlprogramm) und REGUP (bearbeitete Positionen aus Zahlprogramm). Ein Auswertungszugriff ist über die Tabellen BSEC und REGUH/REGUP möglich.

Technische Grundlagen

Es wurden bisher z.B. über Fachartikel in der PRev und Manuals der IBS umfassende Darstellungen zu den FI-Berechtigungsobjekten offeriert[1]. Nachfolgend soll insbesondere die Lieferantenabbildung behandelt werden. Die CpD-Nutzung tritt in den Hintergrund. Sie ist aber datenschutzrechtlich und im Zahlungsbereich auch technisch analog zu sehen.

Im Bereich der Lieferantenabbildung erfolgen die Eingrenzungen auf Berechtigungsobjektebene über die Objekte der Gruppe F_LFA1*. Insbesondere das Objekt **F_LFA1_GRP** (Kreditor: Kontengruppenberechtigung) ermöglicht eine Beschränkung der Zugriffe auf einzelne Kontengruppen, die auf das vierstellig definierte Tabellenfeld LFA1-KTOKK referenzieren. Bei der Auswertung ergibt sich, dass über eine Vielzahl an Kombinationsstandardeinzelrollen, die losgelöst betrachtet als unkritisch gesehen und in vielen Arbeitsplatzrollen gefunden werden können, bis zu mehrere hundert Stammsätze eine Zugriffsmöglichkeit zum Beispiel per Transaktion **FBL1N** (Einzelposten Kreditoren) aufweisen.

<u>Benutzer nach komplexen Selektionskriterien, z.B.:</u>

Berechtigungsobjekt:		F_LFA1_GRP
Feld:		KTOKK – Kontengruppe Kreditor
	Wert:	SONS *(bzw. der für das Unternehmen zutreffende Wert)*
Feld:		ACTVT – Aktivität
	Wert:	03
Berechtigungsobjekt:		S_TCODE
Feld:		TCD-Transaktionscode
	Wert:	FBL1N *(als entsprechendes Beispiel)*

Hinzu kommen die Rollen und Berechtigten, die eine **Tabellensichtfunktion** (z.B. Transaktion SE16, SE16N etc.) und die Tabelleneingrenzung per S_TABU_DIS auf die Gruppe FA (oder S_TABU_NAM bei expliziter Nennung auf die Tabellen) beinhalten.

Sofern also ein Berechtigter beispielsweise die Transaktion FBL1N aufruft und sich die Zahlungen an den gewählten Lieferanten anzeigen lässt (alle Posten), ist er in der Lage, sowohl in der Datumseingrenzung als auch der Höhe des genutzten Ausgleichsbelegs und des Belegpositionstextes (BSEG-SGTXT) die Auszahlungsbeträge zur Person anzeigen zu lassen. Bei entsprechender Berechtigung kann auch auf den FI-Beleg verzweigt werden (FB03), wo wiederum eine Vielzahl zusätzlicher Informationen präsentiert wird.

1 z.B. IBS (2007).

In den Tabellen REGUH und REGUP stehen wiederum die Auszahlungssätze. Die Felder

- LAUFD (als Datumseingrenzung)
- LIFNR (Lieferantennummer)
- VBLNR (Belegnummer des Zahlungsbelegs; Referenz zur BKPF-BELNR/BSEG-BELNR)
- REGUH-NAME1 […]
- ZBUKR (Zahlender Buchungskreis)
- REGUH-XVORL (Nur Vorschlagslauf?; => leer)
- REGUH-ZBNKN (<> leer), -ZBNKL, -ZBNKS, -ZIBAN (Bankverbindungsdaten)
- REGUH-ZALDT (Buchungsdatum des Zahlungsbelegs), -AUGDT (Ausgleichsdatum)
- REGUH-RBETR (Betrag in Hauswährung) bzw. REGUP-DMBTR (Betrag)
- REGUP-SGTXT (Positionstext) und
- REGUP-ZUONR (Zuordnungsnummer)

bilden die Datenbasis für tabellenorientierte Zahlungsdatenauswertungen.

Datenschutzrechtliche Bemerkungen

Die Abbildung dieser Inhalte Im SAP Core ist durchaus sinnvoll. Die Sicht auf Gehaltsdaten des Vorstands als assoziierte Einzelpersonenabbildung ohne nennenswerte Sichtbegrenzung ist im SAP Core zu verhindern. Im HCM ist der Zugriff auf Personalmitarbeiter/-innen restriktiv über Mitarbeiterkreise eingeschränkt. Im SAP Core sollten nur Summensätze auf Kostenstellenebene existieren.

Das Verfahren zur Abbildung und Abrechnung der Aufsichtsratsmandate unterliegt dem Datenschutzrecht[2]. Die DSGVO fordert bereits über die Art der technologischen Implementierung (neue Technologien[3]) und der damit einhergehenden Möglichkeit zur Nutzung der Daten eine Folgenabschätzung der angedachten Verarbeitung zum Schutz der dort prozessierten personenbezogenen Daten. Bereits die Einführung dieses Verfahrens muss nach ehemals § 4d Abs. 5 BDSG (und betriebsrätlich nach § 87 Abs. 1 Nr. 6 BetrVG) einer Vorabkontrolle unterzogen worden sein. Das bisherige BDSG wie auch Art. 35 (3) DSGVO waren bzw. sind bewusst offen formuliert („insbesondere"), sodass auch andere, dort nicht genannte Verarbeitungen einer Datenschutz-Folgenabschätzung (DSFA) zugeführt werden können und sollen. Eine Begrenzung auf ausdrücklich erwähnte Kriterien wäre auch bedenklich, denn dann wäre die korrespondierende Rechtslage, die zu einer etablierten, ergänzenden Bearbeitung zwischen betrieblichem Datenschutzbeauftragten und Betriebsrat geführt hat, ggf. für die Zukunft ausgehebelt. Zu bedenken ist, dass insbesondere die Artikel-29-Gruppe eine Anleitung zur Bewertung von Verarbeitungstätigkeiten erstellt hat, bei denen eine DSFA durchzuführen ist.[4]

Es ist davon auszugehen, dass es sich um personenbezogene Daten zur wirtschaftlichen Nutzung handelt, die insbesondere Aussagen über individuelle Fähigkeiten und Leistungsvermögen zulassen.[5] Valide Bankinformationen, gepaart mit korrekten bzw. aktuellen Adressdaten, sind entsprechend wertvoll. Es besteht grundsätzlich die Gefahr des Kontrollverlustes über diese personenbezogenen Daten. Sie sind nach Art. 9 DSGVO zwar

2 Innerhalb einer Lieferantendatenspeicherung können grundsätzlich auch personenbezogene Ansprechpartnerdaten anfallen. Die datenschutzrechtliche Schutzwürdigkeit über diese Eigenschaft tritt allerdings in den Hinter- und das Charakteristikum des institutionellen Lieferanten dann in den Vordergrund. Die Abbildung der Zahlungsflüsse für Aufsichtsratsmitglieder ist als gesetzlich legitimierte Funktionsausübung anders zu sehen und bei (unternehmensexternen) Mitgliedern die Personenbezogenheit als maßgeblich zu werten.

3 Damit sollte nicht nur gemeint sein, dass Webtechnologien, Vernetzung, Predictive Analytics, Cloud-Datenablage etc. genutzt werden. Auch die Möglichkeit der verbesserten Nutzung von internen Suchalgorithmen über einen Datenbestand sollte diese Bedingung erfüllen. Hinzu kommt, dass sich im Laufe der Zeit Verfahren technologisch anpassen lassen, sodass sie erheblich aufgewertet werden und einer Folgeabschätzung zuzuführen sind.

4 z.B. DSK (2017), auch DIRF (2017). Zur Kritikalität von Bankverbindungsdaten vgl. Wildensee (2010).

5 i.V.m. Art. 4 Nr. 1 DSGVO.

nicht besonders schutzwürdig; da es sich jedoch nicht nur um Personen aus dem Unternehmen, sondern auch um unternehmensfremde Personen handelt, eine explizite Zustimmung zu dieser Verarbeitung im SAP-System wahrscheinlich nicht vorliegt (informierte und dokumentierte Einwilligung[6]), sich die Verarbeitung jedoch aus einer rechtlichen Verpflichtung heraus ergibt[7] (HGB, AktG) und die Verarbeitung systematisch im SAP-System mit integrierter Indexsuchoption stattfindet[8], ist eine DSFA unabdingbar.[9]

Eine rollenbasierte, enge Sichtzugriffsbegrenzung auf diese Stamm- und Bewegungs-/Zahlungsdaten ist als technisch-organisatorische Maßnahme nach Art. 25 und 32 DSGVO naheliegend und aus unserer Sicht zwingend.[10]

Lösungsvariante

Die verschiedenen, aufgabenspezifischen Berechtigungsrollen im Unternehmen haben üblicherweise auf die Lieferantenberechtigungsobjekte F_LFA1* Eingrenzungen, die keine ausreichend separierenden Wirkungen aufweisen. Die Zuweisung der Gruppe SONS (bzw. ein im Unternehmen entsprechend gewählter Wert) in den Stammsätzen der Aufsichtsratsmitglieder führt zu keiner Separierung, da über die Gruppe auch andere Vorgangsarten subsumiert werden, die eine starke Eingrenzung der Zugriffsmöglichkeiten nicht zulassen. Zusätzlich ist zu beachten, dass neben der Tabellenansichtsberechtigung die Retrieval-Funktionen des Systems (z.B. TREX[11]) eine geschäftsprozessbasierte Inhaltssuche ebenfalls zulassen.

Die Lieferantenabwicklung, d.h. Anlage und Bebuchung, ist ein an sich unkomplizierter Funktionsbereich, der im Procure-to-Pay-Prozess zwar ein grundlegender, aber dennoch weitgehend unkritischer Teilprozess ist. Trotzdem ist die Absicherung eine Herausforderung, die viele Baustellen im System aufreißen kann. Es ist die einfachste Lösung, wie oben erwähnt das Berechtigungsobjekt **F_LFA1_GRP** zu nutzen und die Mit-

6 Art. 7 DSGVO: „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. [...] Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. [...]".

7 Art. 6 (1) DSGVO: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. [...]". Zur Datenlöschungsauslegung siehe Art. 17 (3) DSGVO.

8 Art. 35 (1) DSGVO: „Hat eine Form der Verarbeitung, die insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. [...]".

9 Vgl. z.B. auch Erwägungsgrund 75: „[...] oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen [...], persönliche Aspekte bewertet werden, die die Arbeitsleistung, wirtschaftliche Lage [...]".

10 Art. 32 (1) DSGVO: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen [...]". Auch Erwägungsgrund 78: „[...] die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. [..] unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen."

11 Vgl. Schmidt (2017).

glieder des Aufsichtsrates einer eigenen Gruppe (KTOKK) zuzuweisen. Eine Änderung des Abstimmkontos ist dabei nicht notwendig. Dann wird aus jeder Berechtigungsrolle – mit Ausnahme weniger Mitglieder der Buchhaltung, der Revision, des (zentralen) Controllings und ggf. weniger weiterer neuralgischer Punkte im Unternehmen (Anlagerecht sollte ebenfalls stark beschränkt werden) – die Gruppe entzogen. Auch die SAP-Administration benötigt diese Zugriffe nicht. Es ist weiterhin zu prüfen, ob auch die Tabellensichtberechtigungen und Retrieval-Funktionalitäten passend eingegrenzt sind. Hier sollte ein restriktiver Ansatz gefahren werden. Insbesondere auch die direkte Tabelleneinsicht in die REGUH und die REGUP ist zu reduzieren, da hierüber String-basierte Abfragen[12] ermöglicht werden. Dies würde auch ungewollte Analysen im CpD-Bereich erschweren. Letztlich müssen auch die Test-/Integrationssysteme überprüft werden, da diese häufig Systemkopien mit zeitlichem Versatz sind. In den Entwicklungssystemen wiederum können die Entwicklerrollen weiter gefasst werden, wenn hier nicht mit Systemkopien gearbeitet wird.

Abschließend sollte geprüft werden, ob weitere Lieferantenstammgruppen identifiziert werden können, die als Abbildung in vorliegender Form Zweifel aufwerfen. Des Weiteren sollte – unabhängig von dieser Thematik – begutachtet werden, welche Berechtigungsrollen generell über einen Kostenstellenzugriff Einsichtsrechte in Zahlungsflüsse von Einzelpersonen erlauben (z.B. Beauftragte; Objekt K_CCA [Berechtigungsobjekt für Kostenstellenrechnung]; CO_ACTION = 3028 [Einzelposten selektieren], 3029 [Extrakte anzeigen]; KSTAR = *; RESPAREA = Unternehmens- oder entsprechend inkludierte Hierarchie- und Knotenebenen => Transaktionen z.B. OKEN bis OKENNX [Standardhierarchie anzeigen]).

Fazit

Wesentlich sind die Verarbeitungserlaubnis- und Verhältnismäßigkeitsabwägung, die Verfahrensbeschreibung mit Festlegung des benötigten Schutzniveaus (Schadenpotenzial-kategorisiert) und die Technikfolgenabschätzung/DSFA. Analog sollten weitere Personengruppenabbildungen geprüft werden. Trotz der unspektakulären Rechtevergabe und wenig komplexen Rollenausgestaltung an dieser Stelle wird ggf. ein Loch geöffnet, das zwingend zu schließen ist, obwohl es nur ein Sichtrecht ist.

Eine Zusammenarbeit zwischen Revision, betrieblichem Datenschutz und Betriebsrat ist positiv hervorzuheben, da sie zu erheblichen Verbesserungen der Systemsicherheit und der Compliance-Konformität im Unternehmen führen kann.

12 Tabellenfeld SGTXT: Abfrage z.B. like “*vergüt*“, like “*Sitzungsgeld*“ usw.

Literatur

- DIRF (2017): Hinweise zur Datenschutz-Folgenabschätzung nach Art. 35 Datenschutz-Grundverordnung, https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Hinweise_DSFA_20171205.pdf .
- DSK (2017): Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_5_Datenschutz-Folgenabschaetzung.pdf .
- EU-DSGVO (2017): Verordnung (EU) 2016/679 vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de ; https://dsgvo-gesetz.de/erwaegungsgruende/nr-75/ .
- IBS (2007): Prüfen des Einkaufs, IBS Schreiber GmbH, 2. Auflage 2007.
- Schmidt (2017): SAP schließt kritische Lücke in der Search Engine TREX, 13.04.2017, https://www.heise.de/security/meldung/SAP-schliesst-kritische-Luecke-in-der-Search-Engine-TREX-3685632.html .
- Wildensee (2010): Der Zugriff auf wirtschaftlich sensible Kundendaten im SAP, in: PRev III/2010, S. 117–126.

Dr. h.c. **Christoph Wildensee**, DBA, CISM, CRISC, ist seit vielen Jahren in der Internen Revision der enercity AG, Hannover, tätig. Zwischen 2008 und 2012 war er in Personalunion Datenschutzbeauftragter des Unternehmens und der zugehörigen Netzgesellschaft. Er hält einen Doktor ehrenhalber der polytechnischen Universität aus Pernik (EPU).

Dipl.-Kauffrau **Yvonne Wick** ist seit 2011 Revisorin bei der Stadtwerke Gießen AG. Ihre Tätigkeitsschwerpunkte liegen im kaufmännischen Bereich und IT-Prüfungsumfeld.