SAP®-Sicherheit

Christoph Wildensee

Regulatorische Aspekte zur Administration von SAP HCM*

Die Grundlagen der Datenschutzgrundverordnung (DSGVO, GDPR) und der deutschen Umsetzung mit ihren Schutzzielen, limitierend wirkenden organisatorischen Maßnahmen und Begrenzungen der Verarbeitung und Datenweitergabe kümmern sich vornehmlich um die Frage, welche personenbezogenen Daten unter welchen Bedingungen erhoben und was folgend mit diesen passieren darf, ob sie also verarbeitet und weitergegeben werden dürfen, und wie mit bestimmten Gefahrenlagen hieraus umzugehen ist. Was jedoch nie beantwortet wird, ist die Frage, wie viele Beschäftigte bestimmte administrative Aufgaben in den IT-Systemen mit welchen privilegierten Rechten übernehmen dürfen. In kleinen Unternehmen ist dies sicherlich recht leicht zu beantworten, in Großunternehmen allerdings schon aufgrund der Anzahl der IT-Systeme und Komplexitäten nicht. Administratoren müssen besonders auf das Datengeheimnis verpflichtet werden. Sie sind unumgängliche Systemverwalter und Sicherer, dabei immer mit umfänglichen Rechten versehen. Wie viele Beschäftigte jedoch für diese Aufgabe im Unternehmen in einzelnen Systemen benötigt und analog eingerichtet werden, darf das Unternehmen selbst definieren. Es muss lediglich gegenüber dem Landesdatenschutzbeauftragten (vgl. Artikel 57, 58 DSGVO) im Beschwerdefall auf dessen Nachfrage darlegen können, warum es für notwendig erachtet, die Umgebungen so zu wählen, wie sie es ausgeprägt hat (Angemessenheit, funktionale Notwendigkeit, Umsetzung der Schutzziele, Datenschutzfolgeabschätzung).

In jedem Unternehmen gibt es Systeme, die als besonders schutzwürdig deklariert werden, entsprechend sind diese natürlich nach dem **Stand der Technik** abzusichern (vgl. Artikel 32 DSGVO). Dabei geht es sowohl um die Datenklassifizierung/-kritikalität als auch um die Erkenntnisse, die sich aus den

* Aus stilistischen Gründen bzw. zur Vereinfachung der Lektüre wird häufig die männliche Schreibweise verwendet. Die weibliche Form ist jeweils ebenso gemeint und zu bedenken.

Daten ableiten lassen. Aus diesem Gesichtspunkt heraus ist es zunächst gleichbedeutend, ob es sich um ein System zur F&E (ohne nennenswert personenbezogene, aber schutzwürdige Daten) oder um ein Personalabrechnungssystem (mit vielen personenbezogenen Daten je Person, sogar besonderen Arten nach Artikel 9 DSGVO) handelt. Aus der Warte des Unternehmens heraus sollten möglichst wenige Personen aufgabenbezogen mit privilegierten Rechten in einem solchen System versorgt sein. Entsprechend wird häufig bei diesen Funktionen zentralisiert, die Rechteinhaber sollen möglichst nicht zu weit im Unternehmen verstreut sitzen und unter dem Einfluss konkurrierender Bereichsziele agieren müssen. Jedoch steigt die Zahl der Personen im Administrationsbereich stetig an, die wachsende IT-Systemkomplexität mit ihren Schnittstellen/Kommunikationswegen führt zu einer größeren Notwendigkeit, administrative Prozesse dort zu verankern, wo sie aus Sicht des Prozesses zeitoptimiert zugehören. Ein möglicher Zielkonflikt.

Es wird auch unterschieden zwischen ausgesuchten Fachbereichsbetreuern (Key-User, Multiplikatoren) mit durchaus weitreichenden Rechten und administrativen Systembetreuern. Hinzu kommt über die Zeit eine Vielzahl an Beratern und hausfremden Personen, die im Rahmen der Erweiterung des Systemdesigns und/oder der Verarbeitung im Auftrag Zugriffe auf die Systeme erhalten. Zuletzt werden auch im Rollenkonzept zur Verhinderung eines ausufernden Mengengerüstes Rollenbündelungen vorgenommen, sodass mehr Personen auf umfangreiche Zugriffsrechte zurückgreifen können, obwohl dies ggf. nur für wenige Personen mit der zugewiesenen Rolle an der Stelle notwendig ist. Ein solches Vorgehen vereinfacht die Administration und Pflege, verhindert aber zugunsten der wirtschaftlichen Sicht den einengend-schärfenden Datenschutz. Doch dies ist erlaubt und etabliert.

Noch nie wurden Datenskandale aufgrund theoretisch zu umfangreicher Administratorenrechte bekannt. Das Fehlen von Datenschutzbeauftragten in Gesellschaften oder beharrliches Ignorieren behördlich festgestellter, massiver Verfahrensunzulänglichkeiten führte beispielsweise zu Sanktionen. Es gab sie nur aus **nachweislich fehlerhaften Datenverarbeitungen** (auch durch Administratoren), die „**öffentlichkeitswirksam**“ wurden – in dem Sinne, dass das Wissen um das kritisierte Verfahren die Sphäre des Unternehmens verließ.[1] **Doch die theoretisch zu weitreichende Rollenausprägung von IT-Administratoren ohne konkret nachgewiesenen Schaden durch diese wurde noch nie sanktioniert.** Insoweit ist das **Berechtigungskonzept in seiner Ausprägung** zumindest **auslegbar**, der Gedanke der Datensparsamkeit an dieser Stelle nicht im Fokus, denn die Sparsamkeit bezieht sich auf zu verarbeitende Daten und Schlüsse aus der Verarbeitung (vgl. Artikel 5 DSGVO), **kaum auf Rechte zum Zugriff auf die Daten.** Woher kommt nun die Pflicht zum aufgabenbezogen rollenbasierten Berechtigungs- mit abgestuftem Administrationskonzept?

Beim Betrieb von rechnungslegungsrelevanten IT-Systemen sind neben der DSGVO zunächst andere Grundlagen zu beachten, so die Vorgaben aus den **GoBD**, z. B. 3.2.5(58, 59), 6(100), 7(103), 8(110-112), 12(179), und aus den **FAIT-Verlautbarungen**. Beispielhaft seien hier aus FAIT 1 die 3.1(23) mit 4.2(84) aufgezeigt: „[...] Autorisierung bedeutet, dass nur *im Voraus festgelegte Personen* auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das System definierten Rechte wahrnehmen können. Diese Rechte betreffen das Lesen, Anlegen, Ändern und Löschen von Daten **oder die Administration eines IT-Systems**. Dadurch soll ausschließlich die genehmigte Abbildung von Geschäftsvorfällen im System gewährleistet werden. Geeignete Verfahren hierfür sind physische und logische Zugriffsschutzmaßnahmen (z. B. Passwortschutz). Organisatorische Regelungen und technische **Systeme zum Zugriffsschutz sind die Voraussetzung zur Umsetzung der erforderlichen Funktionstrennungen**.“ und „Durch logische Zugriffskon-

1 Zuletzt 2020 ein durch den HmbBfDI verhängter, empfindlicher Bußgeldbescheid an den Bekleidungshändler Hennes & Mauritz wegen der Ausspähung von Beschäftigten in einem Nürnberger Servicecenter. Mindestens seit 2014 wurden heimlich systematische Erfassungen des Privatlebens von Urlaubserlebnissen bis zu Krankheiten/Diagnosen von Beschäftigten zur Profilbildung und arbeitsrechtlichen Verwertung durchgeführt.

trollen z. B. unter Verwendung von Benutzer-ID und Passwörtern ist die **Identität der Benutzer** von IT-Systemen eindeutig festzustellen, um damit nicht autorisierte Zugriffe zu verhindern. **Mitarbeitern sind nur die Berechtigungen zu erteilen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind.** In organisatorischen Grundsätzen sind die Einrichtung, Änderung und Entziehung sowie die Sperrung von Berechtigungen, **die Protokollierung aller Aktivitäten im Bereich der Berechtigungsverwaltung**, die Gestaltung des Passwortes z. B. hinsichtlich Mindestlänge und Ablaufdatum und die **Festlegung von aufgabenbezogenen Berechtigungsprofilen** festzulegen." Hinzugemapped werden über Artikel 32 DSGVO die Referenzbausteine des BSI-Grundschutzes, z. B. vornehmlich OPS.1.1.2 (Betrieb – Ordnungsgemäße IT-Administration), APP.4.2 (SAP-ERP-System) und ORP.4 (Identitäts- und Berechtigungsmanagement); korrespondierende Umsetzungshinweise sind ebenfalls zu beachten.

Der nachfolgende Artikel soll das Thema der privilegierten Rechte im SAP HCM diskutieren.

SAP HCM

Das SAP HCM ist ein führendes System zur Abrechnung der Beschäftigten. Es offeriert allerdings noch eine Vielzahl weiterer Funktionalitäten und kann auch über Drittprodukte mit weiteren Funktionen erweitert werden. Beispiele hierfür sind das Talent Management und die digitale Personalakte. Hinsichtlich der Rechte innerhalb des HCM lässt sich durchaus die Aussage treffen, dass es ein komplexes und schwierig zu durchschauendes System ist. Es weist eine eigene Logikverarbeitung zur Abrechnung von (tarif-) vertraglichen Berechnungen auf. Generell gilt, dass SAP als monolithisches ERP-System trotz seiner Entwicklungen der letzten Jahre berechtigungsseitig sowohl die funktional-operative als auch die Entwicklungs-, Test- und Systemadministrationsebene in einem System beinhaltet. Eine zwingende Trennung dieser Ebenen ist eben nicht vorgeschrieben, jedoch über Systemtrennungen (Produktion, Test/Integration, Entwicklung) und funktional getrennte und privilegiert-protokollierte Stammsätze möglich (vgl. BSI-OPS.1.1.2.A5 und A6). *Doch treffen einzelne Elemente aller Berechtigungsebenen auch im Produktionssystem häufig sich beeinflussend bei den administrativen Funktionswahrnehmungen aufeinander.* Das SAP HCM kann trotz vorhandener Schnittstellen (z. B. zum Core) als Closed-Shop-System betrachtet werden, weil die weitreichenden sowohl manipulativen als auch Sichtrechte auf die kritischen Daten, die als Infotypen separat berechtigt werden können (Basisbezüge [Infotyp 0008], wiederkehrende Be- und Abzüge [Infotyp 0014], Einmalzahlungen [Infotyp 0015], aber auch Behinderungen [Infotyp 0004], Mitarbeiterdarlehen [0045], Darlehenszahlungen [0078] und Daten zu Pfändungen [0111 – 0117], ggf. weitere), nur in wenigen Fachbereichen vorhanden sind. Dies sind die verschiedenen Sachbearbeitungen im Personalbereich (Personalreferent, Abrechnung, Stellenbewertung usw.), ggf. noch per Einsichtsrecht aus der Mitbestimmung heraus der Betriebsrat (Ein-, Umgruppierung, Versetzung, Wiedereingliederung, Behinderung, Gleichstellung etc.). Die System- und Moduladministration und die Systembetreuung im Personalbereich (als Schnittstelle zwischen HR-Anforderungen und SAP-IT-Umsetzung) sollten im Produktionssystem keinen Vollzugriff erhalten. Per Schnittstelle kommen dann noch laufende Datenabgleiche ohne kritische Datenkategorien hinzu, z. B. zwischen HCM und dem führenden Identity Management System.

Funktionale Unterscheidung

In den SAP-Systemen erfolgt die Zugriffssteuerung zweigeteilt. Zum einen benötigt der Anforderer den mit der Programmausführung verknüpften Transaktionscode in seinem

Berechtigungssatz. Hiermit kann er ihn, wenn er ihn aus seiner Rolle heraus aufrufen darf, ausführen, ansonsten erhält er eine ablehnende Hinweismeldung. Nahezu jede Transaktion benötigt jedoch bestimmte klärende Ausprägungen zu Berechtigungsobjekten, die festlegen, welche organisatorischen Objekte der User mit welchem Manipulationsgrad bearbeiten darf. Die Berechtigungsobjekte steuern demnach, in welchem Personenkreis welche Datenkategorien wie verarbeitet werden dürfen. Können beispielsweise die Tarifgruppe oder die Gehaltsdaten angesehen oder auch verändert werden? Organisatorische Zuordnung, familiäre Veränderungen, Steuerklasse, Bankverbindung – alles Daten, auf die unterschiedlich zugegriffen werden kann. Hinzu kommen als dritte Komponente im SAP HCM die strukturellen Berechtigungen [SAP].

Gesteuert wird innerhalb des HCM insbesondere über die Berechtigungsobjekte des P-Kreises. Die Unterscheidung der Zugriffe ist stark abhängig vom Objekt **P_ORGIN** als eines der wesentlichen Objekte. Es kann unterschieden werden, in welchem Personalbereich (T500P; z. B. Gesellschaften) welcher Mitarbeiterkreis (T503K/T503T; z. B. Gehaltsempfänger, Vorstand, leitende Angestellte, Pensionäre) in welcher Mitarbeitergruppe (T501; z. B. aktive, externe) keine, nur lesende oder auch verändernde Zugriffe gestattet sind. Die Transaktionen PA20 oder PA30 (Personalstammdaten anzeigen, pflegen) als Beispiel zeigen dies deutlich. Selbst wenn PA30 im Berechtigungssatz vorhanden ist, ist eine Pflege nicht möglich, wenn nicht in den Berechtigungsobjekten entsprechende Zuweisungen zur Pflege bestimmter Daten vorhanden sind. So ist auch häufig in den Unternehmen festzustellen, dass insbesondere P_ORGIN und P_PERNR (als Objekt, das die Unterscheidung ermöglicht, auch die eigenen oder nur fremde Daten zu pflegen) die eigentliche Unterscheidung des Zugriffs übernehmen, während die meisten anderen Berechtigungsobjekte eine hohe Standardausprägung aufweisen (im Personalbereich sind viele Arbeitsplatzdefinitionen mit vornehmlich pflegenden Berechtigungen mit einem Ausschluss der eigenen Datenpflege anzutreffen; P_PERNR, PSIGN=E). Die Datenpflege erfolgt protokolliert je Änderung.

Rollen der Administration

Zu unterscheiden sind mehrere Administrationstypen, die alle für ihre Tätigkeiten genügend Zeit und Ressourcen benötigen (vgl. BSI-OPS.1.1.2.A1 und A9). Zum einen kommen die Administratoren zum Einsatz, die den laufenden Betrieb des Systems sicherstellen. Diese **Basis- und Datenbankadministratoren** können innerhalb des SAP HCM zunächst sehr gut funktional abgegrenzt werden. Die **P-Transaktionen** können eliminiert, die **P-Berechtigungsobjekte** und **P-Tabellenberechtigungsgruppen** (Tabelle TDDAT) ebenfalls aus dem Berechtigungssatz weitgehend ausgeschlossen werden. Ferner sollten auch grundsätzlich die Objekte

- S_DEVELOP (Development Workbench) mit ACTVT 01, 02, ggf. auch 06, 07 (hinzufügen, ändern, ggf. auch löschen, aktivieren)
- S_SCD0/S_SCD0_OBJ (Änderungsbelege) mit ACTVT 06, 12 (löschen, pflegen)
- S_TABU_DIS (Tabellengruppen) mit ACTVT 01, 02 und DICBERCLS = * bzw. SA/SC/SS (Tabellen der Berechtigungssteuerung)

ausgeschlossen werden; siehe insbesondere GoBD.8(112). Analog darf natürlich auch nicht die Nutzung des Objektes S_TABU_NAM (explizite Tabellennennung) zu einem Aufweichen dieser Zugriffe führen. Auch die Berechtigungsobjekte um S_USER* sollten diese Administratoren nicht aufweisen, sofern es eine IT-gestützte zentrale Rollenbeantragung und -zuweisung gibt (vgl. z. B. BSI-ORP.4.*). Diese Objekte sollten bei den Benutzeradministratoren (Zuweisung Rollen zu Usern) liegen, die nicht als Berechtigungsadministratoren (Rollenbau und -test) arbeiten und auch sonst keine administrativen Aufgaben und Funktionen aufweisen (vgl. BSI-ORP.4.A4 und APP.4.2.A6). Verfolgt man dieses Konzept, wird für mögliche seltene Korrekturen in allen SAP-Systemen jedoch ein

protokollierter Notfalluser benötigt, der diese Ausschlüsse inkludiert und bei Exception genutzt werden kann (vgl. BSI-OPS.1.1.2.A2 und APP.4.2.A29). Die Nutzung dieses Notfallusers sollte bei jedem Einsatz durch die Revision genehmigt und adäquat fallweise durch den nutzenden Fachbereich dokumentiert werden. Dies bedeutet aber auch, dass die Basisadministration diesen Notfalluser ggf. außerhalb des Normpfades nutzen kann, um sich Berechtigungen zuzuweisen. Dies sollte organisatorisch ausgeschlossen werden. Letztlich muss man dieses Restrisiko akzeptieren und durch regelmäßige Checks verproben. Auch der Datenbankadministrator kann letztlich nicht in Zugriffen wirksam eingeschränkt werden, da er außerhalb von SAP auf Datenbankebene einen nahezu Vollzugriff aufweist, benötigt und dies nicht anderweitig limitierend substituiert werden kann. **Dies gilt** allerdings **nicht für HANA**-Datenbanken. Dort besitzt der **Datenbankadministrator per Default keinen Zugriff** auf die ERP/HCM-Daten, da er ihn auch nicht mehr benötigt. Er müsste auch explizit eingerichtet werden. In HANA sind Funktionalitäten wie das DBA-Cockpit generell problematisch, da solche Features ein Sicherheits- und Datenschutzkonzept aushebeln können. Insoweit ist zu prüfen, wo/in welchen Rollenwahrnehmungen solche Zugriffsmechanismen überhaupt Verwendung finden dürfen/sollen.

Zuletzt sei die **Moduladministration** des IT-Bereiches (gleichsam die modulbezogenen Lösungsdesigner im getrennten Entwicklungssystem) zu nennen, die – wie oben eingegrenzt – neben den systemnahen Zugriffen wie SE1*, SE37, SE38, SE80, SE84 usw. ebenso die Modul-P-Transaktionen auch im Produktionssystem benötigt [vgl. WILDENSEE (2014), S. 20]. Nicht nur im Entwicklungs- und Testsystem (häufig mit zeitlichem Versatz kopiertes Produktionssystem, möglichst mit pseudonymisierten Daten pseudonymisiert; vgl. Artikel 4 DSGVO), sondern auch im Produktionssystem ergeben sich für die Moduladministration umfangreiche Rechte. Dies führt letztlich dazu, dass selbst bei ausgesuchtem Fehlen von Rechten innerhalb der Fachfunktion ein Zugriff auf sensible personenbezogene Daten für die Moduladministration möglich ist und kaum wirksam ausgeschlossen werden kann. Trotzdem sollten bestimmte Zugriffe auch für diese Administratoren reglementiert bzw. sogar gänzlich verhindert werden, da hierüber massive datenschutzrechtliche Verstöße möglich sind [vgl. KASTNER (2017)]. Man beachte z. B. die Nutzung von Funktionsbausteinen/BAPIs, die beliebige Personalnummer-individuelle Datenbereitstellungen der Gehaltsabrechnung ausgeben können, siehe z. B. [SAPHRCOMPENDIUM], BAPI_GET_PAY* (teils remotefähig). Dass die Rechte-privilegierte Moduladministration Funktionsbausteine auch für den Fehlerfall im Produktionssystem zumindest testen können muss, ist wohl praxiserprobt (hier S_DEVELOP, ACTVT = 16, OBJTYPE = FUGR, DEVCLASS = PCAL). Dieses Recht sollte trotzdem folgerichtig nur der Notfalluser aufweisen. Modulbetreuer könnten entweder eine Begrenzung erfahren, z. B. ohne PC*, allerdings ist nahezu ausgeschlossen, dass eine umfassende Ausschlussliste mit als kritisch erkannten Klassen vorliegt, sodass dies letztlich doch nur situativ zur Verfügung stehen sollte per Notfalluser, Firefighter o. Ä. (vgl. BSI-APP.4.2.A14). Oder die Aktivität wird in keinem Fall mit 01, 02, 16 belegt. Dies ist im Produktionssystem sicherlich das Sinnvollste. Datenansicht und auch die Manipulationsmöglichkeit über das Testen widersprechen insbesondere auch der GoBD.8.(112). Ein Grund zur Vorsicht besteht auch beim Berechtigungsobjekt S_RFC und bei RFC-Rechten zur Mitnahme von starken Rechten in ein Zielsystem, um dortige Restriktionen zu unterlaufen (keine Trusted-Verbindungen von niedrigen zu höheren Systemen einsetzen). Es ist möglich, diese privilegierten Rechte nur im Bedarfsfall Worklow-basiert – mit der Revision oder dem Personalbereich als Genehmiger – freizugeben. Die Beschränkungen gelten im Übrigen auch für die digitale Personalakte. Der Schlüssel zum Zugriff auf die Akten sollte nur im Personalbereich vorliegen.

Nachfolgend werden zu den Administrationsrollen mögliche Objektausprägungen beispielhaft dargestellt.

Basisadministration	Ausprägung
S_DEVELOP	03|*|*|*|*
S_SCDo / S_SCDo_OBJ	08
S_TABU_DIS	03|A-O, Q-R, T-Z, ggf. 02|A-O, Q-R, T-Z
S_TABU_NAM	./.
S_TABU_SQL	Herausnehmen PA*-Tabellen und Tabellen der Berechtigungssteuerung
S_USER_GRP	*|(ohne ADMIN, SUPER o. Ä.); 03,08|*
S_TRANSPRT	*|*
S_CTS_ADMI	*
P_PERNR	*|*||*
P_ORGIN	*|0105 [Kommunikation]||*|*|*|*
S_TCODE	Keine P-Transaktionen, SU*, SE*, ST*, RZ*, ...
SAP ILM-Berechtigungen	*
Datenbankadministration	**Ausprägung**
S_DEVELOP	03|*|*|*|*
S_SCDo / S_SCDo_OBJ	08
S_TABU_DIS	./.
S_TABU_NAM	./.
S_TABU_SQL	Herausnehmen PA*-Tabellen und Tabellen der Berechtigungssteuerung
S_USER_GRP	./.
S_TRANSPRT	03|*
S_CTS_ADMI	./.
P_PERNR	*|*||*
P_ORGIN	*|0105||*|*|*|*|*
S_TCODE	Keine P-Transaktionen, SU*, SE*, ST*, RZ* ...
Berechtigungsadministration	**Ausprägung**
S_DEVELOP	03|*|*|*|*
S_SCDo / S_SCDo_OBJ	08
S_TABU_DIS	03|A-O, Q-R, T-Z
S_TABU_NAM	02|ZXFT_T_ROLLEN [digitale Personalakte]
S_TABU_SQL	Keine Bereitstellung von Tabellenzugriffen
S_USER_GRP	03,08|*
S_TRANSPRT	03|*
S_CTS_ADMI	./.
P_PERNR	*|*||*
P_ORGIN	*|0105||*|*|*|*|*
S_TCODE	PFCG, sonst nahezu keine P-Transaktionen, SU*, SE*, ST*, ...
HCM-Moduladministration	**Ausprägung**
S_DEVELOP	03|*|*|*|*; 16|*|*|F*,PROG|* => bei ACTVT=16 kritische Funktionsgruppen (DEVCLASS) ausschließen, besser auf diese Definition im Produktions-system verzichten!
S_SCDo / S_SCDo_OBJ	08
S_TABU_DIS	03|*; ggf. 02|* ohne PS,SA,SC,SS,TTRL,SPSE,SPWD, ggf. weitere Gruppen
S_TABU_NAM	./.
S_TABU_SQL	Herausnehmen PA*-Tabellen und Tabellen der Berechtigungssteuerung
S_USER_GRP	03,08|*
S_TRANSPRT	03|*
S_CTS_ADMI	./.
P_PERNR	*|*|E|*

P_ORGIN	*|0001-0003, 0005-0007, 0009-0013, 0016-0044, 0046-0077, 0079-0110, 0118-X999|*|*|*|*|*
S_TCODE	P*, S*, /XFT/*, Z*, ...
SAP ILM-Berechtigungen	*

Tab. 1: Mögliche ausgesuchte Berechtigungsobjektausprägungen der Administrationsebene.

Zuletzt sei der Hinweis erlaubt, dass auch Verzeichnisrechte regelmäßig zu prüfen sind, die Files aus HCM mit personenbezogenen Daten aufnehmen, so z. B. zur Frage, wer den Zugriff auf das Verzeichnis aufweist, in das die Zahlungsverkehrsdateien zur monatlichen Gehaltszahlung geschrieben werden und wer die Erstellung dieser Files durchführt.

Gültigkeitsdauer des Zugriffs

Das Berechtigungsobjekt P_DURATION (Berechtigungszeiträume für HR-Stammdaten) ist ein relativ neues Objekt in der Berechtigungsprüfung für Personaldaten. „Durch die Definition von Berechtigungszeiträumen kann der Zugriff auf Personalstammdaten in die Vergangenheit zeitlich eingeschränkt werden." [MEEDER (2017)] Ist die DURATION abgelaufen, erfolgt kein Zugriff auf die inkludierten Infotypen und die Daten können weder gelesen noch manipuliert werden. Die Prüfung „läuft wie folgt ab: Wenn ein Benutzer einen Report oder eine Transaktion zum Anzeigen oder Bearbeiten von Infotypdaten aufruft, prüft das System, ob für die angeforderten Personaldaten eine Berechtigung aufgrund der organisatorischen Zuordnung des Benutzers vorliegt. Wenn dies der Fall ist, prüft das System, ob die Zugriffsberechtigung für die angeforderten Personaldaten auf Infotyp- oder Subtypebene durch einen Berechtigungszeitraum in Monaten eingeschränkt ist. Dazu liest das System die Einstellungen in der Customizing-Aktivität ‚Default-Berechtigungszeiträume für Infotypen und Subtypen definieren'. Wenn ein Default-Berechtigungszeitraum definiert ist, prüft das System, ob diese Zugriffsberechtigung rollenspezifisch erweitert ist (ID für rollenspezifische Berechtigungszeiträume). Dazu liest das System die Einstellungen in der Customizing-Aktivität ‚Zeitraum-IDs rollenspezifische Berechtigungszeiträume zuordnen'." [CONSOLUT] In vielen Unternehmen ist diese Abgrenzungsfunktion trotz DSGVO-Rechtslage (vgl. Artikel 5 DSGVO und Erwägungsgrund 39, Satz 8) und der Umsetzungsnotwendigkeit der Berichtigung, Sperrung und Löschung personenbezogener Daten allerdings noch gar nicht in der aktiv begrenzenden Nutzung. Dabei ist eine „zeitlich unbegrenzte Aufbewahrung solcher Daten nicht zulässig. Solange [...] gesetzliche, tarifvertragliche oder innerbetriebliche Vorgaben zur Aufbewahrung von personenbezogenen Daten und Unterlagen vorliegen, sind die Daten jedoch noch nicht zu löschen, sondern lediglich zu sperren." [MEEDER (2017)] Die P_DURATION ermöglicht genau das.

Vertrauen in die Administrationsebene

Ein erfolgreiches Administrationskonzept führt an der **Frage des Vertrauens** nicht vorbei.[2] Vertrauen bedeutet hier, dass aufgrund der vorliegenden Ausbildung und der bisherigen Erfahrung mit den Rechte-privilegierten Beschäftigten die subjektive Überzeugung und auch Erwartungshaltung vorherrscht, dass die mit der Wahrnehmung bestimmter

2 „Dabei gilt es zu beachten, dass **Administratoren** hier stets einen besonderen **Vertrauensschutz** besitzen. Dennoch sollten entsprechende Arbeitsanweisungen und Prozesse etabliert sein, welche dazu beitragen, die Vertrauenswürdigkeit des Prozesses zu gewährleisten. So kann etwa durch ein Vier-Augen-Prinzip eine unkontrollierte Änderung durch eine Person vermieden werden. Auch reduziert die Aufteilung von administrativen Tätigkeiten auf mehrere Personen das Risiko. Zuletzt kann über entsprechende Protokollierungen sowie deren regelmäßige Einsichtnahme und Überwachung im Rahmen des IKS eine kompensierende Kontrolle die Prozess-Sicherheit verbessern." GROSS/BRAND/HEINRICH (2017), S. 65.

Rollen und Aufgaben betrauten Personen die daraus bereitgestellten Informationen nicht unsachgemäß durch sie selbst gegen die Interessen des Unternehmens verwenden oder unautorisierten Personen zugänglich machen. Die Administration im HCM-Bereich entspricht einem **erhöhten Schutzbedarf**, der neben genügend Zeit und Ressourcen auch in der **Auswahl des charakterlich passenden Personals** Ausdruck finden muss (vgl. BSI-OPS.1.1.2.A14, A17; BSI-ORP.2.A5, A7). In vielen Häusern hat sich etabliert, dass die Basis- und Datenbankadministration gemeinsam (ggf. gegenseitig vertretend) aus drei bis max. vier Personen (in der Funktion für alle SAP-Systeme; Rufbereitschaft der Basis- und Datenbankadministration beachten; eher Landscape- und Systemgrößen-unabhängig), die Berechtigungsadministration aus zwei (in der Funktion für alle SAP-Systeme) und die HCM-Moduladministration aus zwei bis max. drei Personen bestehen. In größeren Unternehmen wird durchaus auch nach oben abgewichen. Dies sind neuralgische Punkte des Systembetriebs. Sofern die Personen aber über Jahre zusammenarbeiten und bekannt sind, die **Fluktuationsrate gering** ist und diese stark **privilegierten Stammsätze im Produktionssystem** ggf. sogar **protokolliert** werden (zwei Stammsätze je Moduladministrator zur Trennung von persönlichen [z. B. Zeitwirtschaft/ESS] und administrativen Rechten. [Wobei zu fragen ist, wer schaut überhaupt wann in den „Datenfriedhof" der Protokollierung in all seinen Facetten?]; zur Protokollierung z. B. BSI-OPS.1.1.2.A18), kann man davon ausgehen, dass im Umfeld eine geringe Gefahrenlage für maligne Systemzustände, Manipulationsabsichten und unkontrolliertes Data Leakage schutzwürdiger Daten vorliegt. Ein Ausschluss ist dies nicht, fingierte Zugriffsbegründungen sind trotzdem möglich. Die Risikoeinschätzung ist jedoch leichter vorzunehmen – sowohl hinsichtlich der Schadenshöhe als auch insbesondere der Eintrittswahrscheinlichkeit (vgl. auch BSI-APP.4.2., besonders A32, und G 0.32; Artikel 32 DSGVO mit Erwägungsgründen 76-78, 83).

Outsourcing

In vielen Unternehmen wird diskutiert, neben der Bereitstellung der eingesetzten Software und der damit einhergehenden Datenhaltung auch administrative Funktionswahrnehmungen auszulagern (System- und Datenhosting in der Cloud; Funktionsübernahme durch Dienstleister). Regulatorische Grundlagen für die Begutachtung solcher Prozesse sind die Prüfungsstandards des IDW 331 und 951 („Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen" und „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen"). FAIT 1 unter 4.6 ist nach wie vor maßgeblich, so „[…] Wenn die gesetzlichen Vertreter eines Unternehmens betriebliche Funktionen auf ein anderes Unternehmen auslagern (einschließlich IT-gestützter Funktionen), müssen sie die hieraus entstehenden **Auswirkungen auf das interne Kontrollsystem des Unternehmens** beachten. Sofern im Rahmen des Outsourcing die Ausführung von Geschäftsvorfällen und/oder die Datenverarbeitung von einem damit beauftragten Dienstleistungsunternehmen wahrgenommen werden, **verbleibt die Verantwortung** für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen **bei den gesetzlichen Vertretern.** […] muss sich **das Unternehmen die Ordnungsmäßigkeit des internen Kontrollsystems des Dienstleistungsunternehmens nachweisen lassen oder sich Einsichtsrechte vertraglich einräumen lassen**. Für den Fall nicht vertragskonformer Leistungserbringung müssen Einwirkungsmöglichkeiten bis hin zur kurzfristigen Auflösung des Vertrags bestehen." Dies bedeutet nicht selten den mittelfristigen Verlust bzw. zumindest das signifikante Herunterfahren der fachlichen Expertise im eigenen Haus für diesen Funktionseinsatz. Ob den Prüfungserfordernissen nachgekommen wird, ist bis zu einem Schadeneintritt ebenso fraglich. Ein Prüfrecht durch den Auftraggeber sollte zumindest vertraglich eingeräumt werden.

Bei Einsatz eines Dienstleisters ist neben der Kosten- und Zeitersparnisfrage aber auch gar nicht sichergestellt, dass die Aufgabenwahrnehmung nur durch ausgesucht-vertrauenswürdige Personen stattfindet. Vielmehr bekommt der Kunde ggf. gar nicht mit, wer in welchem Zeitraum administrative oder auch manipulative Rechte auf den sensiblen Datenbestand des Kunden erhält (Wer hat z. B. P_ORGIN mit Zugriff auf die Infotypen 0004, 0008, 0014, 0015 […] für welche Aufgaben?). **Bei der Auslagerung besonders sensibler Verfahren** (früher mit/ohne Direktionsrecht des Auftragsgebers als Auftragsdatenverarbeitung/Funktionsübertragung bezeichnet; seit DSGVO nur als Auftragsverarbeitung; der Gerichtsstand des Dienstleisters und der Datenablageort ist dann sehr wohl eine entscheidende Größe), **beispielsweise der Personalabrechnung, kann es maßgeblich sein, wer als Administrator zum Einsatz kommt**. Hierzu BSI-OPS.2.1.A16 bzw. OPS.2.2.A19 für Cloud: „Mit externen Outsourcing-Dienstleistern sollte vertraglich vereinbart werden, dass die **Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft** wird." und „Mit externen Cloud-Diensteanbietern sollte vertraglich vereinbart werden, dass in geeigneter Weise **überprüft** wird, ob das **eingesetzte Personal qualifiziert und vertrauenswürdig** ist." Dies gilt nicht nur für die SAP-Administration, sondern auch für eine ausgelagerte HCM-Personalsachbearbeitung per Business Process Outsourcing (BPO). Dieser deutliche Hinweis zeigt, dass die **Frage des Vertrauens und einer adäquaten Eignungsüberprüfung und Nachweisführung an Wichtigkeit zunimmt** und erkannt wurde. **Ein Freigabe-Veto-Recht, wer welche (administrativen wie auch weitreichenden Sicht- und Manipulations-) Rechte beim Dienstleister auf die Kundendaten erhält, sollte sich der Kunde somit dringend vertraglich einräumen lassen.**

Bei Funktions- oder Verarbeitungsauslagerungen sollte generell hinterfragt werden, ob geschäftskritische, sicherheitskritische oder stark datenschutzrelevante Verarbeitungen in die Hände externer Dienstleister gehören. Dabei ist nicht nur relevant, welche Datenarten/-kategorien gespeichert und wo diese tatsächlich abgelegt werden, sondern auch, wer (auch nur theoretisch) auf diese zugreifen kann (vgl. auch EuGH-Urteil vom 16.07.2020). Eine Auslagerung kann rechtlich zulässig, jedoch trotzdem die falsche Entscheidung sein.

Fazit

Es ist durchaus ableitbar, welche Rolle Administratoren im Unternehmen spielen, welche Rechte sie in welchem System benötigen, in welchen sie beschnitten werden sollten und wie viele Personen mit welchen Skills (Eignung fachlich wie charakterlich) diese Rolle ausüben müssen. In dieser Arbeit weitgehend unbetrachtet bleibt die gesetzlich nicht verankerte, jedoch über Artikel 32 DSGVO legitimierte und etabliert-wirkstarke „best practice"-Literatur. Weder aus dem Handels- und Steuerrecht, noch aus dem Datenschutzrecht heraus gibt es eine aktive Diskussion um das Thema Vertrauen, jedoch wird im Rahmen der Definition der technisch-organisatorischen Maßnahmen (TOMs) und der Erreichung der Kontrollziele auch geschaut werden müssen, **wie für die Garantie der gesetzeskonformen Umsetzung durch das Unternehmen gegenüber externen Anspruchsberechtigten geworben wird** (Datensparsamkeit, Definition der TOMs nach Stand der Technik, Leitfädenbeachtung, BSI-Grundschutz u. a.). Ein Faktor ist dabei sicherlich auch die Frage, kann ich der administrativen Ebene, die unbestreitbar notwendig ist, grundsätzlich vertrauen, sowohl was den Funktionsumfang als auch die persönliche Integrität bis zur Anzahl der Personen betrifft. Konkreter wird es hinsichtlich dieser Fragestellung an kaum einer anderen Stelle (eher sich in Nuancen wiederholend), weder in Gesetzen noch in Standards.

Für die Revision sind dieses Verhältnis und seine Interpretationsgrundlage relevant, wenn sie mit den Bereichen auf Augenhöhe Risikoeinschätzungen diskutieren möchte.

Nur bei entsprechender Awareness hinsichtlich dieser Punkte und einem korrespondierenden Maß an Kontrolle, das aufgrund der Revisionskapazitäten gar nicht erschöpfend sein kann, können gemeinsam gute Lösungen zur Data Leakage/Data Loss Prevention entwickelt werden.

Literatur

BSI Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_Uebersicht_node.html; Umsetzungshinweise, z. B. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/OPS/Umsetzungshinweise_zum_Baustein_OPS_1_1_2_Ordnungsgem%C3%A4%C3%9Fe_IT-Administration.html

CONSOLUT (o.J.): P_DURATION – Berechtigungszeiträume für HR Stammdaten, https://www.consolut.com/s/sap-ides-zugriff/d/e/doc/YK-P_DURATION/

EUGH (2020): Lesetipp zum EuGH-Urteil: EU/US-Privacy Shield ist unwirksam – Was Unternehmen jetzt wissen müssen; https://drschwenke.de/eugh-urteil-eu-us-privacy-shield-unwirksam/; http://curia.europa.eu/juris/liste.jsf?num=C-311/18

FAIT 1 (2002): IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) , http://www.weg-mit-dem-papier.de/files/pdf/FAIT1.PDF

GROSS/BRAND/HEINRICH (2017): Die GoBD in der Praxis – Ein Leitfaden für die Unternehmenspraxis – Version 2.3, 13. März 2017.

HANDELSBLATT (2020): Mitarbeiter ausgespäht: Datenschutzbeauftragter verhängt Rekord-Bußgeld gegen H&M, https://www.handelsblatt.com/unternehmen/handel-konsumgueter/modehaendler-mitarbeiter-ausgespaeht-datenschutzbeauftragter-verhaengt-rekord-bussgeld-gegen-hundm/26234570.html?ticket=ST-1126830-spCY4scNlZYB1QgABOip-ap5; 01.10.2020.

KASTNER (2017): Begrenzter Zugriff für Basisbetreuer, https://e-3.de/begrenzter-zugriff-fuer-basisbetreuer/

MEEDER (2017): Löschen und Sperren personenbezogener Daten im SAP HCM, Björn Meeder, IBS Hamburg, 2017, https://e-3.de/loeschen-und-sperren-personenbezogener-daten-im-sap-hcm/

SAP (o.J.): Zusammenwirken von allgemeinen und strukturellen Berechtigungen, https://help.sap.com/erp_hcm_ias_2013_01/helpdata/de/00/bcb83b5b831f3be10000000a114084/content.htm

SAPHRCOMPENDIUM (o.J.): SAP HR Collections – Entire HR in SAP at a glance – BAPI, https://saphrcompendium.wordpress.com/technical/bapi/

WILDENSEE (2014): Zugriffsberechtigungen/Access Management in rechnungslegungsrelevanten SAP ERP-Systemen: Exemplarische Rechtsgrundlagen, Risiken und Lösungsansätze für die kommunale deutsche Energiewirtschaft, 2014.

Christoph Wildensee, DBA, CISM, CRISC, CDPSE, 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.