1. Hintergrund

Die Notwendigkeit für ein SAP-bezogenes „Protokollierungs- und Kontrollkonzept“ leitet sich unter anderem aus verschiedenen gesetzlichen Normen ab.[1]

Nach der EU-Datenschutzgrundverordnung[2] (kurz: DSGVO) sind im Zusammenhang mit dem geforderten Schutzniveau von personenbezogenen Daten entsprechende Sicherheitsmechanismen einzurichten. Dazu zählt auch die Protokollierung und Überwachung von sicherheitsrelevanten mit einer Person in direkter Verbindung stehenden Aktivitäten in einem SAP-System.[3] Die über eine Protokollierung z.B. identifizierten, kritischen Sicherheitsverstöße sind dementsprechend nachzuverfolgen. Da derart generierte Protokolldaten personenbezogene Daten enthalten können, ist neben dem Nachweis der Zweckbindung[4] der Zugriff auf diese Daten entsprechend einzuschränken.

Die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (kurz: GoBD[5]) fordern an mehreren Stellen[6] eine „Revisionsfähigkeit“ der abgebildeten Sachverhalte oder der vorgenommenen Änderungen, die üblicherweise durch die Maßnahme der Protokollierung umgesetzt wird.

Unabhängig von dem Schutzbedarf personenbezogener Daten ist eine Protokollierung von relevanten Ereignisse aber auch für die Überwachung von (SAP-) Systemfunktionen und der (SAP-) Sicherheit zwingend erforderlich. So kann ein aktivierte Protokollierung sowohl dazu beitragen, potentielle Schwachstellen frühzeitig zu erkennen und damit auch frühzeitig zu beseitigen als auch Verstöße gegeen Sicherheitsvorgaben zu erkennen oder Nachforschungen zu einem eingetretenen Sicherheitsvorfall zu ermöglichen (z.B. Wer hat wann die „hochsensiblen“ Unternehmensdaten kopiert?).

In einem Konzept sind grundsätzlich vor der Umsetzung beispielsweise festzulegen, welche Protokolldaten in einem SAP-System generiert werden sollen, welche Monitoring-Werkzeuge zur Auswertung der Daten verwendet werden sollen sowie wer für die Ininiierung bzw. für die Umsetzung verantwortlich ist. Letztendlich ist auch zu bestimmen, wie der „laufende“ Prozess zur Protokollierung und Überwachung auszugestalten ist.

Mit der Umsetzung der DSVGO ändern sich auch die „Nachweispflichten“ der Unternehmen grundlegend. So bezieht sich die geforderte „Rechenschaftspflicht“ („accountability“, Art 5 Abs. 2 DSGVO) nicht nur auf die Zuständigkeit und Verantwortung für die Einhaltung der festgelegten Grundsätze zur Datenverarbeitung (Art. 5 Abs. 1 DSGVO) sondern auch auf die Nachweispflicht für Unternehmen. Demnach **muß** ein Unternehmen gemäß Art. 5

---

[1] Siehe auch Abschnitt Nr. 5. Normative Anforderungsgrundlagen, Seite 5.

[2] Hier insbesondere die Artikel 24 und 32.

Die **Verordnung (EU) 2016/679** des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (kurz: Datenschutz-Grundverordnung, DSGVO) löst die **Datenschutzrichtlinie 95/46/ EG** von1995 (im Folgenden: Datenschutzrichtlinie) ab. Im Unterschied zur Datenschutzrichtlinie gilt die DSGVO unmittelbar in der gesamten Europäischen Union (Art. 288 Abs. 2 AEUV).

Das **BDSG n.F**. behandelt sogenannte in der DSGVO vorgesehene „Öffnungsklauseln“ und umfasst damit nur solche Regelungsbereiche, die nicht durch die DSVGO abgedeckt werden.

[3] Quelle: SAP-Berechtigungswesen – Konzeption und Realisierung, Lehnert, Stelzner, Otto, John, 3. Aktualisierte Auflage von 2016.

[4] Dabei ist mit der Einführung der DSGVO ab Mai 2018 durch die Unternehmen explizit nachzuweisen, dass die Protokollierung ausschließlich dem Zweck der Aufrechterhaltung von Datenschutz und Datensicherheit dient und dass diese nicht zum Zweck einer automatisierten Verhaltens- und Leistungskontrolle der Beschäftigten genutzt wird.

[5] Siehe Details: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile (Aufruf am 8. Mrz. 2018).

[6] Siehe auch z.B. Unveränderbarkeit (Tz. 59), Historien für Bewegungs- und Stammdaten (Tz 89), Unveränderbarkeit, Protokollierung von Änderungen (Tz. 111).

Abs. 2 DSGVO nachweisen, dass es als „Verantwortlicher" angemessene und wirksame Maßnahmen (Art. 24 Abs. 1 DSGVO) ergreift, um die datenschutzrechtlichen Grundsätze und Verpflichtungen der DSGVO umzusetzen. Hieraus können wieder verschiedene Vorgaben für die Protokollierung und Überwachung abgeleitet werden.

Bei der Planung und Erstellung eines „Protokollierungs- und Kontrollkonzeptes" sind aufgrund der möglicherweise generierten personenbezogenen Protokolldaten daher auch datenschutz- und betriebsverfassungsrechtliche Fragestellungen zu berücksichtigen.

Hinweis

Das SAP-bezogene „Protokollierungs- und Kontrollkonzept" ist ein Teil eines **übergeordenten Protokollierungs- und Kontrollkonzepts**, in dem Protokollierungen auch bei anderen, für den SAP-Betrieb aber wesentliche IT-Komponenten und –Infrastruktur behandelt werden (z.B. Netzwerkzugriffe).

2. Geltungsbereich (Rev.)

Die im Zusammenhang mit dem SAP-Protokollierungs- und Kontrollkonzept nachfolgend dargestellten SAP-Soll-Vorgaben sind grundsätzlich für alle Prüfungen des SAP-Protokollierungs- und Kontrollkonzeptes in der Diehl-Gruppe – ergänzend zu den bereits vorhandenen Vorgaben - heranzuziehen.

3. Definitionen

Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.[7]
SAP-Basis-System	Das SAP-R/3-**Basis**-System ist eine Art „Betriebssystem des SAP-R/3-Systems, das aus „**logischer Sicht**[8]" den sogenannten „Kernel", verschiedene (Basis-) „Dienste" sowie weitere „Komponenten" wie die ABAP-Workbench und die Präsentationskomponente umfasst. Diese als „Kernel & Basisdienste" zusammen-

[7] Art. 4 Nr. 1 DSGVO bzw. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU).

[8] Die logische Sicht auf ein SAP-R/3-System unterscheidet sich z.B. von einer hardware- oder softwaretechnischen Sicht dahingehend, dass die hierunter aufgeführten Komponenten nicht unbedingt einer spezifischen Hardware- oder Software-Einheit zugeordnet werden können.

gefasste Komponente dient als hardware-, betriebssystem- und datenbankunabhängige Ausführungsumgebung[9] aller R/3-Anwendungen.[10]

Aus Software-technischer Sicht kann ein SAP-System in drei „Schichten“ aufgeteilt werden: Datenbank, Applikation und Präsentation.

Datenbank (Datenhaltung)

- Die Datenbank liegt i.d.R. auf einem Datenbankserver. Die Zugriffe und Administration werden über ein Datenbankmanagementsystem[11] vorgenommen.
- Die Datenbank enthält neben den Bewegungs- und Stammdaten eines SAP-R/3-Systems auch sowie zahlreiche Systemdaten (Customizing, Programmcode, etc.).
- Es wird zwischen Datentabellen oder Systemsteuertabellen unterschieden.
- Die SAP-Anwendungsprogramme greifen im Rahmen ihrer Funktionen auf die Datenbank lesend und schreibend zu.
- Die für die Kommunikation zwischen den einzelnen System-Schichten und für die Kommunikation mit dem Systemumfeld erforderlichen Schnittstellen sind in der Datenbank definiert und hinterlegt.

Applikation (Anwendung)

- Diese Schicht stellt die Kernkomponente eines SAP R/3-Systems dar und enthält die eigentliche „Logik“ (Geschäftslogik) z.B. für die Abbildung der einzelnen Geschäftsprozesse.
- Diese Schicht kommuniziert in beide Richtung, sowohl an die Präsentationsschicht als auch an die Datenbankschicht.
    - Mit den Anwendungsprogrammen (z.B. SAP-FI/CO) auf den Applikationsservern werden die benötigten Daten aus der Datenbankschicht

[9] In der Ausführungs- bzw. Laufzeitumgebung werden wiederum einzelne SAP-R/3-Anwendungen ausgeführt, Benutzer und Prozesse verwaltet, Datenbankzugriff und die Kommunikation mit anderen SAP-Systemen koordiniert. Des Weiteren enthält die Komponente Programme, die es erlauben den laufenden Betrieb eines R/3-Systems zu überwachen, zu steuern und Laufzeitparameter zu verändern.

[10] Das SAP-Basis-System mit seiner Ausführungsumgebung ist wiederum als „Anwendung“ unter einem anderen Betriebssystem wie z.B. Microsoft Windows installiert.

[11] Ein Datenbanksystem wird in der Regel in eine „Datenbank“ und in ein „Datenbankmanagementsystem“ unterteilt. Das Datenbankmanagementsystem (DBMS) ist die eingesetzte Software, die für das Datenbanksystem installiert und konfiguriert wird. Das DBMS legt das Datenbankmodell fest und übernimmt dabei einen Großteil der gestellten Anforderungen an ein Datenbanksystem wie z.B. das Speichern, Überschreiben und Löschen von Daten, das Verwalten von Metadaten aber auch die Gewährleistung der Datensicherheit und der Datenintegrität oder Vorkehrungen zum Datenschutz.

	angefordert, verarbeitet, für den Nutzer aufbereitet und an die Präsentationsschicht weitergegeben. o Die Daten, die der Anwender in die Benutzeroberfläche „SAP-GUI“ („Präsentationsschicht“) eingibt, werden wiederum über die Applikationsserver in die Datenbank „geschrieben“. • Ein Applikations-Server kann mehrere Workprozesse gleichzeitig zur Verfügung stellen („Parallelisierung“). **Präsentation** • Die Präsentationsschicht ist die oberste Schicht des R/3 SAP-Basis Systems und umfasst die Kommunikation mit dem Anwender bzw. Benutzer. • Hierfür werden die angeforderten Daten mittels Softwarekomponenten aus den Anwendungsprogrammen der Applikationsschicht für den Nutzer am Endgerät graphisch aufbereitet. • Die Präsentationssschicht stellt somit die Schnittstelle zu den Anwendern bzw. Benutzern dar („SAP-GUI) .
Drei-System-Landschaft	SAP-System-Verbund bestehend aus einem „Entwicklungssystem“ („DEV“), einem „Qualitätssicherungssystem“ („QAS“) und einem „Produktivsystem“ („PRD“). Das Entwicklungssystem enthält beispielsweise einen Customizing-Mandanten, das Qualitätssicherungssystem einen Qualitätssicherungsmandanten und das Produktivsystem einen Produktivmandanten.
Leseprotokollierung	Verfahren mit dem Zweck die Nachvollziehbarkeit von Lesezugriffen auf Daten durch Mitarbeiter sicherzustellen (Teil der Zugriffskontrolle). In bestimmten Situationen ist gesetzlich vorgeschrieben, dass Lesezugriffe auf sensitive bzw. sensible Daten nachweisbar zu protokollieren sind. In SAP existiert mit dem sogenannten Read-Access-Logging (RAL) eine technische Möglichkeit, die lesenden Zugriffe auf definierte Daten umfassend und selektiv zu protokollieren.[12]
Besondere Arten / Kategorien personenbezogener Daten[13]	Synonyme sind „sensitive“ bzw. „sensible Daten“. Nach der Definition des Bundesdatenschutzgesetzes

[12] Über den SAP Read-Access-Logging-Framework können Protokollierungsregeln nicht nur auf Datenbank- oder Feld-Ebene definiert werden, sondern es können beispielsweise Einschränkungen der Protokollierung auch auf Basis des Feldinhalts vorgenommen werden (um z.B. nur Lesezugriffe auf einige definierte Datensätze einer Tabelle zu protokollieren).

[13] Siehe hierzu auch: Art. 9 Abs. 1 DSGVO und „Datenschutz mit SAP“ von Lehnert, Luther, Christoph, Pluder, SAP PRESS, S, 37f.

§ 3 Abs. 9 BDSG a.F. bzw. Richtlinie (EU) 2016/680[14] gehören dazu folgende Datenarten:

- Angaben über die rassische und ethnische Herkunft,
- Angaben über politische Meinungen,
- Angaben über religiöse oder philosophische Überzeugungen,
- Angaben zur Gewerkschaftszugehörigkeit,
- Angaben über Gesundheit,
- Angaben zum Sexualleben.
- Angaben zu religiösen oder weltanschaulichen Überzeugungen,
- Genetische Daten,
- Biometrische Daten.

4. Zielsetzung

Mit dem Erstellen bzw. Pflegen eines Protokollierungs- und Kontrollkonzeptes sind grundsätzlich nachfolgende **Zielsetzungen** verbunden:

- Einhaltung gesetzlicher Anforderungen,
- Gewährleistung der – teilweise gesetzlich geforderten – Nachvollziehbarkeit,
- Gewährleistung der Datenintegrität,
- Gewährleistung der Überprüfbarkeit der Wirksamkeit von Datenschutzkontrollmaßnahmen,
- Frühzeitige Erkennung und Beseitigung von potenziellen Schwachstellen,
- Erkennen von Verstößen gegen Sicherheitsvorgaben

5. Normative Anforderungsgrundlagen

1. GoBS, GDPdU (bis 2014),
2. GoBD (ab 2014),[15]
3. HGB, KonTraG
4. Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW, PS 330),
5. BDSG a.F. (insbesondere § 31 und Anlage zu § 9 BDSG[16]),
6. BDSG n.F. (Anforderungen aus der „Datenschutzgrundverordnung“ (DSGVO), ab 25. Mai 2018),
7. Datenschutzleitfäden der Deutschsprachige SAP® Anwender-gruppe (DSAG) e. V,
8. Prüfleitfäden der Deutschsprachige SAP® Anwender-gruppe (DSAG) e. V.

[14] Siehe auch DSGVO.

[15] Beispiel: Vorgaben zur Stammdaten-Protokollierung.

[16] Technisch organisatorische Maßnahmen, kurz: TOM’s.

6. Verantwortlichkeiten

Die Verantwortung für die Initiierung, Erstellung und konkrete Ausprägung eines SAP-Protokollierungs- und Kontrollkonzeptes obliegt regelmäßig dem **IT-Sicherheitsbeauftragten**, der **Datenschutzbeauftragen** und dem **IT-Leiter**. Der **Fachbereich** hat hierbei ein **Mitwirkungspflicht**.
Die Verantwortung für die Umsetzung des Konzeptes liegt regelmäßig bei dem zuständigen (System-) **Administrator**.
Die konkreten Verantwortlichkeiten sind mit den eineindeutigen Funktionsnamen im Konzept aufzuführen.

7. Mindestanforderungen[17]

7.1. Vorgabe ist vorhanden

Ein aktuelles, schriftliches und entsprechend freigegebenes, datenschutzkonformes Protokollierungs- und Kontrollkonzept liegt für alle SAP-Systeme und alle darin enthaltenen Mandanten vor.

Hinweis I

Es müssen Vorgaben zu den wichtigsten Protokollen in einem SAP-System enthalten sein.

7.2. Formale Kriterien werden erfüllt

Das Protokollierungs- und Kontrollkonzept erfüllt folgende **formalen Anforderungen** bzw. **Dokumentationsstandards**:

• **Geltungsbereich**	Der Geltungsbereich des Protokollierungs- und Kontrollkonzeptes ist definiert.
• **Überprüfung**	Festlegung eines Turnus und der Verantwortlichkeit für die regelmäßige Überprüfung des Protokollierungs- und Kontrollkonzept auf Aktualität und Richtigkeit.
• **Schriftform**	Das Protokollierungs- und Kontrollkonzept liegt in Schriftform vor.
• **Freigabe**	Das Protokollierungs- und Kontrollkonzept ist entsprechend freigegeben.
• **Aktualität**	Das Protokollierungs- und Kontrollkonzept ist aktuell.
• **Kommunikation**	Das Protokollierungs- und Kontrollkonzept wurde an die relevanten Stellen kommuniziert.

Das schriftliche Protokollierungs- und Kontrollkonzept muss derart verfasst sein, dass es

- verständlich, zuverlässig bzw. verlässlich und richtig sowie überprüfbar und
- „ordnungsgemäß“ gemäß den zugrundeliegenden rechtlichen Normen ist. Die Ordnungsmäßigkeit ist gegeben, wenn die
  - Einhaltung gesetzlicher Anforderungen,
  - Gewährleistung der – teilweise gesetzlich geforderten – Nachvollziehbarkeit,
  - Gewährleistung der Datenintegrität,

[17] Die Mindestanforderungen basieren sowohl auf gesetzlichen Vorgaben u. Normen als auch auf Leitfäden von Fachgremien, (IT-) Fachverbänden und Berufsverbänden.

- Gewährleistung der Überprüfbarkeit der Wirksamkeit von Datenschutzkontrollmaßnahmen, frühzeitige Erkennung und Beseitigung von potenziellen Schwachstellen, sowie das
- Erkennen von Verstößen gegen Sicherheitsvorgaben

gegeben ist.

7.3. Inhaltliche Mindestvorgaben

In einem SAP-System können die bestehenden Protokollierungsmöglichkeiten grundsätzlich folgenden drei Gruppen zugeordnet werden:

- Technische Protokolle,
  (z.B. SysLog, Security Audit Log, Tabellenprotokollierung, etc.)
- Anwendungsprotokolle,
  (z.B. Änderungsbelegschreibungen, Aufzeichnung der Starts von Reports, Infotypbelegschreibung, etc.)
- „Spuraufzeichnungen“ (traces).
  (z.B. SAP-System-Trace, Systemlastmonitor, Performance-Trace, Nutzungsstatistik, etc.)

Insbesondere bei Protokollierungen von personenbezogenen Daten sollte das Protokollierungs- und Kontrollkonzept Vorgaben neben der Art und dem Umfang der Protokollierung auch Angaben zur jeweiligen Zweckbindung[18] bzw. Zielsetzung (z.B. Auswertung der Nutzungsstatistik zur Verbesserung der aufgabenbezogenen Berechtigungen) und zum genauen Inhalt der Protokollierung machen.

Das Protokollierungs- und Kontrollkonzept sollte **mindestens** nachfolgende inhaltliche bzw. technische Vorgaben enthalten:

Hinweis
Die nachfolgende Aufzählung ist nicht abschließend. Die Umsetzung der aufgeführten Vorgaben ist abhängig von dem jeweilig betrachteten SAP-System (→ **ohne** HCM oder **mit** HCM).

[18] Siehe hierzu auch das DIG-interne Dokument „Datenschutzgerechte Protokollierung“ (DIG-RL-020, 2015, Ansprechpartner Herr Dr. Buss).

1. **SysLog (Systemprotokoll)**

   Protokollierung aller systemrelevanten und definierten sicherheitsrelevanten Vorgänge.

2. **Security Audit Log**

   Das Protokollierungs- und Kontrollkonzept enthält bezogen auf das Security Audit Log Vorgaben zu

   - **Aktivierung**

     Hinweis

     Das Security Audit Log muss aktiviert sein, um damit Benutzeraktivitäten - wie z.B. solche von Notfall-Benutzern - protokollieren zu können.

   - **Mindesteinstellungen**

     Definition der zu protokollierenden
     - Benutzer,
     - Audit-Klassen und
     - Ereignisse.

     Hinweis

     Für alle Notfallbenutzer werden alle Ereignisse aller Audit-Klassen protokolliert (siehe auch Notfall-Benutzer-Konzept).

   - **Verantwortlichkeiten**

     Definition der Verantwortlichkeiten für die Einrichtung und Änderung der Einstellung des SAP Security Audit Log.

3. **Versionshistorien**

   Protokollierung der Änderungen an Programmen und am Data Dictionary

4. **Änderungsbelege**

   Protokollierung der Änderungen an
   - Rollen,
   - Stamm- und Bewegungsdaten.

5. **Protokollierung von Tabellenänderungen**

   Über Tabellenänderungsprotokolle wird die gesetzlich geforderte
   - Nachvollziehbarkeit von Änderungen[19] im Customizing in rechnungslegungsrelevanten SAP-Systemen,
   - Zweckgebundenheit des Zugriffes auf personenbezogene Daten sichergestellt.

   Im Rahmen des Protokollierungs- und Kontroll-Konzeptes ist daher festzulegen, für welche Tabellen eine Änderungsverfolgung aktiviert werden soll.

   Hinweis

   Folgende Protokollierungen sind zu aktivieren
   - Protokollierung der Änderungen am Customizing,
   - Protokollierung der gemäß SAP-Hinweis 112388 protokollierungspflichtigen Tabellen sowie weiterer rechnungslegungsrelevanter Tabellen. Dies kann gegebenenfalls auch eigenentwickelte Tabellen betreffen,
   - Protokollierung aus IKS-Sicht (z.B. SAP-Tabelle DD09L und DEVACCESS).

[19] Änderungen, die im produktiven SAP-System vorgenommen werden, unterliegen zu Nachweiszwecken der eingesetzten Verfahren bestimmten Protokollierungsanforderungen. Diese Anforderung ergibt sich aus § 238 HGB ff. Hierfür stellt SAP einige „Mechanismen“ an, mit deren Hilfe Kontrollen ermöglicht werden, die Risiken aufdecken („detektive Kontrollen“) und minimieren können. Mögliche Risiken können u.a. aus fehlender Funktionstrennung oder aus Fehlern bei der Stammdatenpflege resultieren.

6. Protokolle zur Benutzerverwaltung

Protokollierung der Änderungen an Benutzern

- Anlage von Benutzern,
- Änderung von Benutzern,
- Zuweisung von Rollen.

7. Protokolle zur Systemänderbarkeit

Protokollierung der Änderungen an den Einstellungen der Systemänderbarkeit.

8. Zugriffsstatistik

Protokollierung der Aufrufe von Transaktionen, Reports sowie Funktionsbausteine von Benutzern.

9. Lesezugriffsprotokollierung (Read Access Logging)

Als eine Maßnahme zur Sicherstellung und Gewährleistung der gemäß Datenschutz (technisch-organisatorische Maßnahmen) geforderten „Zugriffskontrolle“ ist auch die Nutzung bzw. Aktivierung der Lesezugriffsprotokollierung zu rechnen.

Da die Leseprotokollierung eine Art „Verhaltenskontrolle“ darstellt, unterliegt sie den Mitbestimmungsrechten des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG.[20]

Das heißt vor Aktvierung bzw. Einrichtung der Lesezugriffsprotokollierung ist die Zustimmung des Betriebsrates und auch die des Datenschutzbeauftragen einzuholen.

Im Rahmen des Protokollierungs- und Kontrollkonzeptes sind bezogen auf das Read Access Logging mindestens Vorgaben zu folgenden Punkten zu treffen:

- Verwendung bzw. Aktivierung der Lesezugriffsprotokollierung
- Daten, die im Rahmen des RAL zu protokollieren sind
  Hinweis: Die Lesezugriffsprotokollierung ist i.d.R. auf besonders sensible Daten und Angaben zu Bankkonten zu beschränken.
- Definition und Beschreibung der Verfahren zur Auswertung der Zugriffsprotokolle

10. Festlegung der Protokollierung in HCM u.a.

- Protokollierung der Reportstarts HCM
- Änderungsbelege HCM-Infotypen
- Protokollierung und Überwachung von:
  - Tabellenänderungen
    - an HCM-Customizing-Tabellen (eingeschlossen unternehmenseigener Tabellen
    - an den PA-Tabellen
  - HCM--Reports (einschließlich unternehmenseigener Reports)
  - Stammdatenänderungen (sog. Infotyp-Protokollierung)
  - Lesezugriffsprotokollierung (Read Access Logging)
- Gegebenenfalls Berücksichtigung von besonderen Anforderungen bei der Protokollierung von sensiblen bzw. sensitiven Daten (s.a. Abschnitt 3. Definitionen, Seite 2)

[20] Hierzu sind unter Umständen auf Konzern-Ebene weitere Maßnahmen zu ergreifen.

11. Definition der Speicher- bzw. Aufbewahrungsorte für die erzeugten Protokolle

Hinweis:

Revisionssichere Speicherung bzw. Aufbewahrung.[21]

12. Festlegung der Aufbewahrungsfristen bzw. Löschfristen

Die erzeugten Protokolle müssen gemäß den gesetzlichen Anforderungen vorgehalten werden und sofern erforderlich, wieder lesbar gemacht werden können.

Aus diesem Grund ist die Definition und Festlegung von Aufbewahrungsfristen im Rahmen des Protokollierungs- und Kontrollkonzeptes erforderlich.[22]

13. Vorgaben zur Zugriffsberechtigung auf die erzeugten Protokolle[23]

Hinweis

Technische Sicherstellung, dass Protokolle im Nachhinein nicht durch IT-Administratoren geändert werden können.

14. Definition und Festlegung der Kontrolle der erzeugten Protokolle

Dabei vorab definieren, wie die Auswertungs- bzw. Überwachungsroutinen inhaltlich ausgestaltet werden sollen („Wer wertet wann welche Daten wie und unter welchem Aspekt aus?“). Gegebenenfalls ist ein Vier- bzw. Sechs-Augen-Prinzip (bei z.B. Anfangsverdacht auf dolose Handlungen, u.U. Einbezug Betriebsratvertreter).

[21] „Revisionssicher“ als synonym für eine verfälschungssichere, langzeitige Archivierung elektronischer Informationen.

[22] Unter Umständen ist hierzu eine konzernübergreifende Regelung erforderlich.

[23] Siehe auch entsprechende Unterlage zu Rollen- bzw. Berechtigungskonzept.

8. Reports, Transaktionen und Tabellen

Bei den nachfolgend nicht abschließend aufgeführten (SAP-) Reports, Transaktionen und Tabellen ist zwischen folgenden inhaltlichen Zielstellungen zu unterscheiden:

- Vornehmen von Protokollierungseinstellungen,
- Kontrolle bzw. Überwachung und Auswertung der generierten Protokolldaten.

Report, Transaktion, Tabelle	**Beschreibung**
SM21	Auswertung des SystemLog
SM19	Konfiguration des Security Audit Log
SM20 / SM20N	Auswertung des Security Audit Log
SM30_V_T585A, SM30_V_T585B, SM30_V_T585C	Einstellung der Protokollierung der Infotypen (Tabelle T585A, T585B und T585C)
SE03	Administration/Systemänderbarkeit
SE11	ABAP Dictionary Pflege Einstellung der Protokollierung von Tabellenänderungen in einem Mandanten
SE13 / SE13A	Dictionary: Technische Einstellungen Einstellung der Protokollierung von Änderungen für einzelne Tabellen
SPAM	Support Package Manger
SRALMANAGER	Read Access Logging Manager
SRALMONITOR	Monitor für die Lesezugriffsprotokollierung
SUIM	Benutzerinformationssystem
RFKABL00	Änderungsanzeige Kreditoren
RFDABL00	Änderungsanzeige Debitoren
RDDPRCHK	Customizing-Tabellen ohne Protokollierung (alternativ: SE16→DD09L)
RPUPROTD	Protokoll der Reportstarts HCM
RPURPOTU	Löschen der Protokolle der Reportstarts
RPUAUD00	Änderungsbelege HCM-Infotypen
RPUAUDDL	Löschen der Protokolle zu Infotyp-Änderungen
RSCD0K91 RSCD0K95 RSCD0K99	Löschen von Änderungsbelegen („Wer kann diese Reports ausführen?)

Report, Transaktion, Tabelle	Beschreibung
RSSCD100	Änderungsbelege anzeigen (z.B. für Rollen)
RSTBHIST	Auswertung der Tabellenprotokollierung inkl. Historie, Auflistung der protokollierten Tabellen und Versionsvergleiche
RSUSR100 / RSUSR100N	Änderungsbelege für Benutzer
RSVTPROT	Auswertung der Protokolle der Tabellenänderung

♦ ♦ ♦