Pseudonymisierung und Datenauskunft (DSGVO)

Webdesk bietet zwei Werkzeuge für den Datenschutz (DSGVO): die **Pseudonymisierung** aller Personen im System (z.B. bevor eine Datenbankkopie zur Fehleranalyse weitergegeben wird) und den **Export aller personenbezogenen Daten einer einzelnen Person** (Auskunftsrecht, Art. 15 DSGVO). Die Seite richtet sich an Administratoren und Consultants. Die Pseudonymisierung wird im Administrationsmenü bzw. unter *Erw. Funktionen* ausgeführt, der Datenexport als Bericht im HR-Expert (Voraussetzung: HR-Modul, siehe Allgemeines zu HR-Expert[1]).

Achtung: Die Pseudonymisierung wirkt auf **alle Personen des Systems** und löscht die Audit-Trail-Daten unwiderruflich (siehe Abschnitt "Warnungen und Risiken"). Sie ist für Test- und Kopiesysteme gedacht, nicht für das Livesystem.

Überblick und Abgrenzung

Werkzeug	Zweck	Wo
Pseudonymisierung	Ersetzt bzw. entfernt identifizierende Daten aller Personen. Die Originalwerte werden verschlüsselt im System abgelegt und können wiederhergestellt werden.	Maske "Pseudonymisierung (DSGVO)"; Aktionen unter "Erw. Funktionen"
Datenexport einer Person	Liefert alle gespeicherten personenbezogenen Daten einer Person als Bericht (Auskunft nach Art. 15 DSGVO). Verändert keine Daten.	HR-Expert, Menü "Berichte", Eintrag "DSGVO Persönliche Daten"

Die Pseudonymisierung ist **keine Löschung**: Personen bleiben mit ihrer Struktur (Gruppenzuordnungen, Buchungen, Workflows) erhalten, nur die im Schema genannten Felder werden verändert. Die Löschung von Personen nach einer Aufbewahrungsfrist erfolgt über eigene Jobs (siehe Job PoDeletePersonsAfterYears[2]; Austritte werden vom Job ProcessTerminatedEmployees[3] verarbeitet). Im Code gibt es keine Kopplung zwischen diesen Jobs, dem Papierkorb und der Pseudonymisierung.

Pseudonymisierung

Zweck und Einsatz

Laut Beschreibung der Maske dient die Pseudonymisierung dazu, Personendaten DSGVO-konform zu pseudonymisieren, bevor eine Kopie zum Zweck der Fehlerbehebung weitergegeben wird. Typischer Ablauf: Datenbank des Livesystems auf ein Testsystem kopieren, dort pseudonymisieren, erst danach die Kopie weitergeben.

Was die Pseudonymisierung leistet:

- Namen, Benutzername, Kontaktdaten, Geburtsdatum, Bankverbindungen, Bilder und weitere HR-Stammdaten werden laut Schema ersetzt oder entfernt.
- Die Aktion ist wiederholbar: bereits pseudonymisierte Personen werden übersprungen, sofern sich das Schema nicht geändert hat.
- Die Originalwerte werden verschlüsselt im System gespeichert (Protokoll der Pseudonymisierung, je Person und Entität). Dadurch ist eine Wiederherstellung möglich.

Was sie **nicht** leistet:

- Es werden nur die im Schema aufgeführten Felder behandelt. Alle anderen Daten bleiben unverändert, z.B. Passwörter (nicht Teil des Standardschemas), Workflow-Daten und Formularinhalte, Logs, Dateien und Dokumente. Zusätzliche Behandlungen gibt es nur für Notizen und das Zeitsystem (siehe unten).
- Es handelt sich nicht um eine Anonymisierung: die Originaldaten liegen verschlüsselt weiterhin in der Datenbank.

Standardschema: welche Felder werden wie verändert

Die Schemata sind als Spring-Beans PoPersonDefaultPseudonymizationConfig (PO) und HrPersonDefaultPseudonymizationConfig (HR) ausgeliefert. Ein in der Maske gespeichertes Schema hat Vorrang vor dem Standard-Bean.

Person (PoPerson)

Feld	Ergebnis	Strategie
userName	Zufällige Buchstabenfolge (15 Zeichen), die im System noch nicht vorkommt. Hat der Mandant ein Benutzernamen-Präfix, wird es vorangestellt (Bean PoPseudonymizeUsernameWithPrefix). Die Anmeldung ist danach nur mit dem neuen Benutzernamen möglich.	CUSTOM_HANDLER
firstName, lastName	Zufälliger Vor- bzw. Nachname, der bei einer anderen Person des Systems vorkommt. Vor- und Nachname werden unabhängig gewürfelt. Es entstehen also Namen, die tatsächlich im Unternehmen existieren.	RANDOMIZE
cellPhoneNumber	Konstante +43 676 123 4567	CONSTANT
dateOfBirth, email	Wert wird geleert	DELETE
bankAccounts, personImages	Alle Bankverbindungen bzw. das Personenbild werden gelöscht	DELETE

HR-Person (HrPerson, nur mit HR-Modul)

Alle folgenden Felder werden mit DELETE geleert bzw. ihre Einträge gelöscht: birthName, ethnicCode, privatePhoneNumber, privateCellPhoneNumber, comment, privateEmail, socialSecurityNumber, contactAddresses, contactInstantMessagings, contactWebProfiles, relatives, internalRelatives, secondaryJobs, priorEmployments, personMaritalStatuses.

Die zur HrPerson gehörende PoPerson (gleiche ID) wird dabei mit ihrem eigenen Schema (Tabelle oben) mitbehandelt.

Zusätzliche Aufgaben

Aufgabe (Bean)	Wirkung	Wann aktiv
"Pseudonymisieren der Notizen von Personen" (PoQuickNotePseudonymizationTaskHandler)	Der Text jeder Notiz der Person wird durch Blindtext (Lorem ipsum) fester Länge ersetzt.	Im Standardschema der PoPerson enthalten

"Pseudonymisiere Personen im Zeit System" (TaPersonPseudonymizationTasklet Handler)	Hat die Person eine TA-ID, werden Name, Vorname und Nachname des Personensatzes im Zeitsystem (TA-Connector) auf die pseudonymisierten Werte gesetzt. Andere Zeitwirtschaftsdaten werden nicht verändert. Ist der Connector nicht erreichbar, wird dieser Schritt mit einer Warnung im Log übersprungen. Bei der Wiederherstellung wird der Name im Zeitsystem wieder angeglichen.	Wird bei Aufruf der Pseudonymisierung automatisch ergänzt, wenn das TA-Modul vorhanden ist

Verschleierungsstrategien

In der Maske kann je Feld eine der folgenden Strategien gewählt werden.

Eigenschaft	Erklärung	mögliche Wert(e)
CONSTANT	Das Feld erhält den angegebenen konstanten Wert (Spalte "Custom Bean/Constant Value"; bei Datumsfeldern ein Datum im Format dd.MM.yyyy).	beliebiger Wert
RANDOMIZE	Das Feld erhält einen Wert, der in diesem Feld bei einer anderen Person desselben Typs vorkommt (bis zu 10 Versuche, einen vom aktuellen verschiedenen Wert zu finden; sonst Zufallstext bei Textfeldern bzw. leerer Wert).	-
RANDOMIZE_UNIQUE	Das Feld erhält eine zufällige, im System noch nicht vorhandene Buchstabenfolge (15 Zeichen). Nur für Textfelder. Wird nach 10 Versuchen kein freier Wert gefunden oder ist das Feld kein Text, wird der Wert leer.	-
DELETE	Bei Listen (z.B. Bankverbindungen) werden alle Einträge gelöscht, bei einfachen Feldern wird der Wert geleert.	-
CUSTOM_HANDLER	Der Wert wird von einer Spring-Bean berechnet, deren Name in der Spalte "Custom Bean/Constant Value" angegeben wird.	Beanname (z.B. PoPseudonymizeUsernameWithPrefix)

Ausführen

Es gibt zwei Einstiege. Beide verarbeiten **alle Personen**; mit HR-Modul wird bei den HrPerson begonnen, ohne HR-Modul bei den PoPerson. Die Verarbeitung erfolgt in Blöcken zu je 100 Datensätzen.

Variante A: Maske "Pseudonymisierung (DSGVO)"

Menü Administration > System > Sicherheit > "Pseudonymisierung (DSGVO)" (in der Menüvorlage full-admin direkt unter "System"). Die Maske zeigt oben den Status "System ist pseudonymisiert" bzw. "System ist nicht pseudonymisiert".

Eigenschaft	Erklärung	mögliche Wert(e)
Entität	Wählt das Schema, das angezeigt und bearbeitet wird.	PoPerson; HrPerson (nur mit HR-Modul)
Zusätzliche Pseudonymisierungsaufgaben	Liste der zusätzlichen Aufgaben (Spalte "Zusätzliche Aufgaben") für die gewählte Entität.	Notizen von Personen; Personen im Zeit System
Feld Regeln	Tabelle mit den Spalten "Feldname", "Verschleierungsstrategy" und "Custom Bean/Constant Value". Zeilen können hinzugefügt und gelöscht werden.	siehe Verschleierungsstrategien

Schaltflächen: Speichern, Speichern und Schließen, **"Speichern und Anwenden der Pseudonymisierung"** (Warn-Symbol) und Zurück.

1. Sicherstellen, dass es sich um ein Test- bzw. Kopiesystem handelt und ein Datenbank-Backup vorliegt.
2. Maske öffnen, Entität wählen und bei Bedarf die Feld Regeln anpassen.
3. "Speichern und Anwenden der Pseudonymisierung" klicken. Gespeichert wird das Schema der gerade gewählten Entität; danach läuft die Pseudonymisierung aller Personen im Hintergrund mit Fortschrittsanzeige.
4. Nach Abschluss die Maske neu öffnen und prüfen, dass der Status "System ist pseudonymisiert" lautet. Der Status gilt nur dann, wenn für jede Person ein Protokoll vorhanden ist. Lautet er weiterhin "nicht pseudonymisiert", sind einzelne Blöcke fehlgeschlagen (siehe Warnungen).
5. Audit-Trail wieder aktivieren, falls er benötigt wird (siehe Warnungen).

Hinweis: Das in der Maske gespeicherte Schema ersetzt für diese Entität das ausgelieferte Standard-Bean. Wurde noch nichts gespeichert, wird das Standard-Bean verwendet.

Variante B: Aktion unter "Erw. Funktionen"

Menü Administration > System > "Erw. Funktionen", Bereich "Modulspezifische Aktionen". Im Auswahlfeld erscheinen die Aktionen in der Gruppe "Personalwesen":

- **"Standard-Pseudonymisierung auf HrPerson-Entitäten anwenden"** (Klasse HrApplyDefaultPseudonymizationOnHrPerson)
- **"Pseudonymisierte HrPerson-Entitäten wiederherstellen"** (Klasse HrApplyRestoreOnPseudonymizedHrPerson)

Aktion wählen, "Führe Aktion aus" klicken und im Dialog "Modulspezifische Aktion ausführen" bestätigen. Der Dialog zeigt die Beschreibung der Aktion. Eine eigene Warnung für zerstörerische Aktionen wird für diese beiden Aktionen nicht angezeigt. Trotz der Bezeichnung "Standard" verwendet die Aktion das aktuell wirksame Schema (ein in der Maske gespeichertes Schema, sonst das Standard-Bean). Auch hier läuft die Verarbeitung für alle Personen; es gibt keine Fortschrittsanzeige.

Wiederherstellen

Die Wiederherstellung ist nur über die Aktion "Pseudonymisierte HrPerson-Entitäten wiederherstellen" möglich (die Maske hat keine Wiederherstellen-Schaltfläche). Sie liest die verschlüsselten Originalwerte aus dem Protokoll, schreibt sie in die Felder des Schemas zurück und löscht danach das Protokoll der Person. Für Personen ohne Protokoll passiert nichts.

Daten	Verhalten bei der Wiederherstellung
Einfache Felder (Namen, Benutzername, Telefon, E-Mail, Geburtsdatum, ...)	Originalwert wird zurückgeschrieben. Zwischenzeitliche Änderungen dieser Felder werden überschrieben.
Gelöschte Listen (Bankverbindungen, Kontaktdaten, Angehörige, Nebenbeschäftigungen, ...)	Die Einträge werden mit den gesicherten Werten als **neue Datensätze** angelegt (neue interne IDs).
Notizen, Namen im Zeitsystem	Text bzw. Name wird zurückgesetzt.
Audit-Trail	Nicht wiederherstellbar (bei der Pseudonymisierung gelöscht).

Ohne HR- bzw. ohne TA-Modul

- Ohne HR-Modul wird nur die PoPerson-Entität verarbeitet (Standardschema oben). Die HR-spezifischen Felder existieren dann nicht. Die Maske bietet nur die Entität PoPerson an. Dass die Maske auch ohne HR-Lizenz aufrufbar ist, wurde mit Version 4.59.27 korrigiert (siehe Release Notes 4.59.27[4]).
- Ohne TA-Modul entfällt der Abgleich mit dem Zeitsystem.

Export aller personenbezogenen Daten einer Person (Art. 15 DSGVO)

Berechtigung und Ort im Menü

- Bericht **"DSGVO Persönliche Daten"** im HR-Expert, Menü **"Berichte"**.
- Der Bericht (Konfiguration exportAllPersonalGDPRData) ist standardmäßig der Standardrolle HR_ADMIN zugeordnet, also den HR-Expert-Benutzern (z.B. Rolle $HRX_User). Bei bestehenden Installationen wurde die Standardrolle durch ein Update-Skript nachgetragen.

Durchführung

1. Im HR-Expert Menü "Berichte" > "DSGVO Persönliche Daten" öffnen.
2. Als Parameter (PersonUID) die betroffene Person auswählen (Auswahl aus den Personen, angezeigt wird der vollständige Name).
3. Ausgabeformat wählen. Konfiguriert sind HTML-Ansicht, PDF, Excel und Druck. Im Excel-Export steht jede Tabelle auf einem eigenen Blatt.
4. Bericht ausführen und das Ergebnis prüfen. Die Weitergabe an die betroffene Person sollte über einen sicheren Kanal erfolgen.

Inhalt des Berichts

Der Bericht beginnt mit dem Namen der Person und, falls vorhanden, dem Personenbild.

Abschnitt	Inhalt	Voraussetzung
"Persönliche Daten"	Alle befüllten Felder der HR-Person, in der Reihenfolge der Personen-Maske. Listenwerte (Schlüsselwerte) und Auswahlwerte erscheinen übersetzt, Datumswerte als yyyy-MM-dd.	HR-Modul
Tabellen der HR-Person	Je Liste der HR-Person (z.B. Kontaktdaten, Angehörige) eine	HR-Modul

	Tabelle mit den Spalten, die in der Personen-Maske für diese Liste konfiguriert sind. Leere Listen entfallen.	
"Protokollierung von Informationen"	"Protokollierte Aktionen": Aktion, Mobile Browser, Start/Ende, IP, Browser Benutzer Agent, URL. "Login Versuche": Datum, IP, Resultat, Browser Benutzer Agent.	immer; Einträge nur, wenn vorhanden
"Zeiterfassung"	"Anwesenheitsinformationen": Anwesenheit, Ganzer Tag/Halber Tag, Intervall, ab Beginn der Zeiterfassung bis heute.	TA-Modul; Person mit TA-ID
"Reiseinformation"	Reisen: Von, Bis, Reise Nr., Reise-Typ, Zielort, Gesamt ohne Steuern, Total, Status.	TM-Modul
"Workflow-Anfragen"	Vom Benutzer gestartete Workflow-Anfragen: Process Name, Name der Prozessdefinition, Prozessinstanz-ID, Status, Erstellt, Datum der letzten Aktivität.	WF-Modul
"Projekte"	Zeitaufwände ab Gültig-ab der Person bis heute: Datum, Von/Bis, Dauer (Minuten), Beschreibung, Projekt, Aktivität, Kunde, Verrechenbar.	PTM-Modul
"Umplanungen"	Planungen: Datum, Von/Bis, Dauer, Ganztägig umplanen, Planungs Titel, Planungen (Struktur).	RS-Modul

Hinweis: Der Umfang der Abschnitte "Persönliche Daten" und der Tabellen der HR-Person richtet sich nach der Formulardefinition der HR-Person für den Mandanten der Person. Felder, die in dieser Maske nicht vorgesehen sind, erscheinen nicht im Bericht.

Daten, für die im Bericht kein Abschnitt vorgesehen ist (z.B. Dokumentenverwaltung, Groupware/Kalender, Notizen, Audit-Trail-Einträge), müssen bei Bedarf gesondert ermittelt werden.

Warnungen und Risiken

- **Achtung:** Nicht auf dem Livesystem ausführen, außer dies ist ausdrücklich gewollt. Die Aktion betrifft immer *alle* Personen; es gibt keine Auswahl einzelner Personen. Vorher ein Datenbank-Backup erstellen.
- **Achtung:** Zu Beginn der Pseudonymisierung wird der Audit-Trail **deaktiviert** (Systemparameter HibernateAuditTrailInterceptor, Eigenschaft active wird auf false gesetzt) und seine Tabellen werden gelöscht und neu angelegt, weil sie personenbezogene Daten enthalten können. Die bisherigen Audit-Trail-Einträge gehen unwiderruflich verloren. Auch die Wiederherstellung stellt sie nicht wieder her und aktiviert den Audit-Trail nicht erneut. Bei Bedarf die Eigenschaft nachher wieder auf true setzen.

- **Achtung:** Fehler in einzelnen Verarbeitungsblöcken (je 100 Datensätze) werden nur im Log auf Debug-Ebene vermerkt, die Verarbeitung läuft weiter und es kann trotzdem eine Erfolgsmeldung erscheinen. Danach immer den Status in der Maske und stichprobenartig Personen prüfen.
- **Achtung:** Schema nicht zwischen Pseudonymisierung und Wiederherstellung ändern. Die Wiederherstellung arbeitet mit dem aktuell wirksamen Schema. Felder, die erst später ins Schema aufgenommen wurden, haben keinen gesicherten Originalwert und können dadurch geleert werden; Felder, die aus dem Schema entfernt wurden, werden nicht zurückgeschrieben. Wird das Schema geändert, während Personen bereits pseudonymisiert sind, stellt die Pseudonymisierung diese Personen zuerst wieder her und wendet dann das neue Schema an.
- **Achtung:** Pseudonymisierte Namen sind echte Namen anderer Mitarbeiter (RANDOMIZE). Das ist für Tests gewollt, kann aber im Testsystem zu Verwechslungen führen. Benutzernamen werden zufällig ersetzt, Passwörter bleiben unverändert. Für Kopiesysteme bietet sich zusätzlich "Alle Passwörter zurücksetzen" an (siehe Erweiterte Funktionen[5]).
- **Hinweis:** Eine weitergegebene Datenbankkopie enthält weiterhin die verschlüsselten Originalwerte (Protokoll der Pseudonymisierung). Sie ist damit pseudonymisiert, nicht anonymisiert.
- **Hinweis:** Nach der Wiederherstellung neu angelegte Listeneinträge haben neue interne IDs. Verweise auf die alten IDs (z.B. aus Importen) gehen ins Leere.

1. /daisy/personalwolke-admin/7588-dsy.html
2. /daisy/personalwolke-admin/9259-dsy.html
3. /daisy/personalwolke-admin/7475-dsy.html
4. /daisy/personalwolke-admin/11219-dsy.html
5. /daisy/personalwolke-admin/463-dsy.html