VOMATEC®

ARIGON® PLUS

Personenbezogene Daten in ARIGON® PLUS

Inhaltsverzeichnis

Personenbezogene Daten

1.1 Rechtliche Legaldefinition

Personenbezogene Daten sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“, § 3 Abs. 1 BDSG. Dabei wird eine Identifizierbarkeit einer natürlichen Person auch dann angenommen, wenn diese indirekt zu mehreren besonderen Merkmalen identifiziert werden kann (Art. 4 Nr. 1 DS-GVO).[1]

1.2 Personenbezogene Daten in ARIGON® PLUS

In ARIGON® PLUS werden personenbezogene Daten werden über Feuerwehr-, Werksangehörige und sonstige Personen, die für die Abwicklung von Sicherheitsaufgaben benötigt werden, gespeichert. Nachfolgend wird, entsprechend der obigen Legaldefinition, unterschieden zwischen direkten und indirekten personenbezogenen Daten.

1.3 Direkte personenbezogene Daten

Beispiele:

- Name, Geburtsdatum, Adresse, Erreichbarkeiten, Beruf
- Abteilungszugehörigkeit, Dienstgrad, dienstliche Ehrungen, Beförderungen
- Funktionen in der Feuerwehr, überörtliche Funktionen
- arbeitsmedizinische Untersuchungen (ohne Untersuchungsergebnis, nur Tauglichkeits-feststellung), vorhandene Impfungen
- Fahrerlaubnis, erhaltene persönliche Ausstattung/Persönliche Schutzausrüstung
- Arbeitgeber, Angehörige (als Verständigungsadressen im Einsatzfall bzw. bei Unfällen), Bankverbindung (für Kostenerstattung u. Ä.)
- Fortbildungen, Lehrgänge – einschließlich Anmeldung, Stundennachweise (für Kosten-erstattung oder Nachweis von Übungs- oder Einsatzstunden)

Der jeweilige Lizenznehmer (Behörde, Feuerwehr, Verwaltung, Betrieb, …) muss für sich festlegen, wer welche Zugriffsrechte auf die personenbezogenen Daten hat.
ARIGON® PLUS bietet hierzu eine komplexe Berechtigungsstruktur, um diese Daten vor unberechtigtem Zugriff zu schützen.

1.4 Indirekte personenbezogene Daten

Als indirekte personenbezogene Daten werden Bewegungsdaten einer natürlichen Person verstanden, die Rückschluss auf Nutzungsverhalten des Systems erlauben.

Beispiele:

- Zeitstempel der letzten erfolgreichen Anmeldung des Benutzers
- Zeitstempel der letzten Fehlanmeldung des Benutzers
- Erstellungs-/Änderungszeitstempel zu einem Datensatz
- Systemprotokoll-Aufzeichnungen

[1] Auszug aus „Datenschutzrecht“, 9. Auflage 2017, Beck-Texte im dtv, Seite XXXIII.

- Benutzerprotokoll-Aufzeichnungen

Der jeweilige Lizenznehmer (Behörde, Feuerwehr, Verwaltung, Betrieb, …) muss für sich festlegen, ob die Erhebung der indirekten personenbezogenen Daten für einen reibungslosen Betriebsablauf benötigt wird. Für die erhobenen Daten muss der Lizenznehmer weiterhin festlegen, unter welchen Aufbewahrungsfristen und Datensicherungsmaßnahmen die Daten zu speichern sind. Für die innerhalb ARIGON® PLUS gespeicherten Daten können Zugriffs- und Löscheinstellungen vorgenommen werden. Für außerhalb ARIGON® PLUS gespeicherter Datensätze, z.B. Benutzerprotokoll-Exporte, liegt die Fürsorgepflicht vollständig beim Lizenznehmer, da ARIGON® PLUS auf diese Daten keinen Verwaltungszugriff hat.

1.5 Besonders sensible personenbezogene Daten

Nach Art. 9 DS-GVO gelten bestimmte personenbezogene Daten als besonders schützenswert. ARIGON® PLUS sieht nicht vor, solche besonders sensiblen personenbezogenen Daten zu verwalten.

1.6 Schutzziele personenbezogener Daten

Die Einhaltung der rechtmäßigen Erhebung und Verarbeitung, der Zweckbindung sowie der Einhaltung des Prinzips der Datenvermeidung und Datensparsamkeit Personenbezogener Daten innerhalb ARIGON® PLUS obliegt dem Lizenznehmer. ARIGON® PLUS bietet Funktionen zur Erhebung und Verwaltung der Daten, unterlegt mit technischen Datensicherheitsmechanismen. Datensicherheitsmechanismen werden in ARIGON® PLUS stetig ausgebaut, um das Schutzziel zu erfüllen.

1.7 Abgrenzung

ARIGON® PLUS kann technisch nicht prüfen, ob personenbezogene Daten in Freitextfeldern (z.B. Bezeichner, Freitextinhalte, Freitextprotokollierungen) oder innerhalb von Dokumenten enthalten sind. Entsprechend sind für diese im Allgemeinen keine gesonderten Regelungen getroffen. Nur für automatisiert überführte sensible Daten in solche Freitextfelder, ist dies in diesem Dokument hervorgehoben (z.B., wenn eine Person als Lagerort definiert wird).

1.8 Auftragsdatenverarbeitung

Personenbezogene Daten in ARIGON® PLUS verbleiben beim Lizenznehmer in ARIGON® PLUS. Es findet im Regelbetrieb kein Datenabgleich oder Datenaustausch statt.

1.9 Ausnahmen

Ausnahmen dieser Regelung sind gegeben unter folgenden Bedingungen:

1. Der Lizenznehmer betreibt explizit eine Schnittstelle (ARIGON® PLUS Interface) zu einem externen Gewerk, über die Personenbezogene Daten abgeglichen werden. Zum Beispiel ein Abgleich mit einer Telefonbuch-Software.
2. Zur Ursachenanalyse und Behebung eines gemeldeten Systemfehlverhaltens werden die Datensätze (DB-Dump) vom Lizenznehmer an VOMATEC übertragen.

Für Ausnahme 1. obliegen die Einhaltung der Schutzziele und Rechtmäßigkeit dem Lizenznehmer.

Für Ausnahme 2. obliegt die Datenverarbeitung dem Erlaubnistatbestand zur Erfüllung vorvertraglicher Pflichten oder zur Vertragsdurchführung, im Rahmen von z.B. Support- und Wartungsverträgen. Die Daten werden bei VOMATEC gesichert behandelt und mit Wegfall des Erlaubnistatbestandes (Abschluss der Analyse, Behebung der jeweiligen Meldung) gelöscht.

2 Rollen und Rechtekonzepte

2.1 Benutzer

Für jeden ARIGON® PLUS Anwender wird ein Benutzer in ARIGON® PLUS angelegt. Die Authentifizierung erfolgt über die Kombination aus Benutzer und Passwort. Das Passwort wird generell verschlüsselt dargestellt. Sollten das Passwort vergessen werden, gibt es keine Möglichkeit dieses zu lesen. Es kann muss ein neues Passwort vergeben werden.

Benutzer in ARIGON® PLUS können vom Systemverwalter aktiviert bzw. deaktiviert werden (Ankreuzfeld „Anmeldung erlaubt“). Ebenso kann die Anzahl von Anmeldefehlversuchen optional eingeschränkt werden (brute force prevention).

Zur Erhöhung der Sicherheit bei der Benutzerauthentifizierung können in ARIGON® PLUS Passwortrichtlinien eingestellt werden.

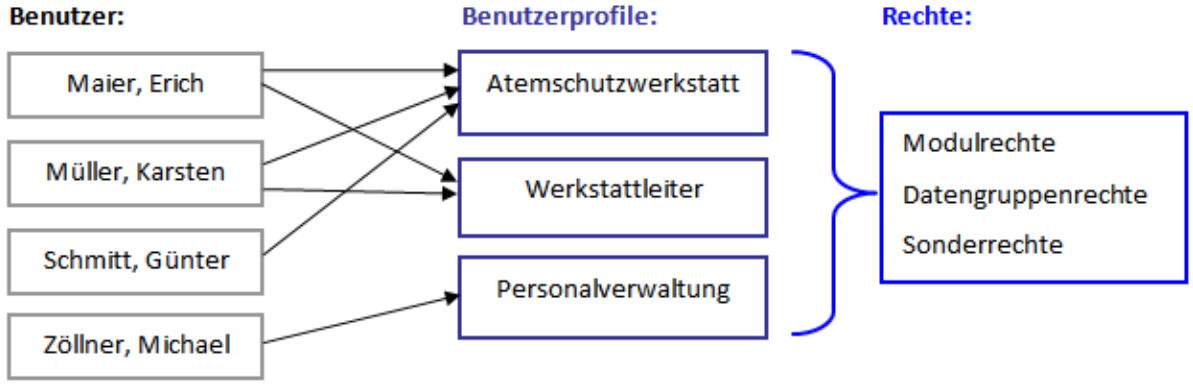
Passwortregeln		
Mindestanzahl große Buchstaben	0	0
Mindestanzahl kleine Buchstaben	0	0
Mindestanzahl Sonderzeichen	0	0
Mindestanzahl Ziffern	0	0
Mindestlänge	0	0

2.2 Rollenkonzept

Rollen werden in ARIGON® PLUS durch Benutzerprofile realisiert. ARIGON® PLUS bietet die Möglichkeit, für beliebig viele Benutzer Profile mit unterschiedlichen Rechten einzurichten. Die Anzahl ist nicht durch die Lizenz begrenzt.

2.3 Rechtekonzept

Die Zugriffsrechte der Benutzer (Anwender) werden in so genannten Benutzerprofilen festgelegt. Der Benutzer kann verschiedene Profile erhalten. Die Rechte aller seiner Profile werden addiert. Dabei ist vorgesehen, alle Bearbeitungen mit getrennten Benutzern vorzunehmen, da zu jedem Datensatz (Material, Person, ...) gespeichert wird, welcher Benutzer diesen Datensatz zuletzt an welchem Datum bearbeitet hat. Sie können gezielt in den Daten nach diesen Informationen suchen.



Innerhalb des Benutzerprofils werden über die Verknüpfungen in der Modulleiste verschiedene Zugriffsrechte zusammengestellt. Sollen mehrere Anwender unterschiedliche Rechte bekommen, müssen auch mehrere Benutzerprofile angelegt werden. Neu erfasste Benutzerprofile haben zunächst keine Berechtigungen. Die Berechtigungen umfassen:

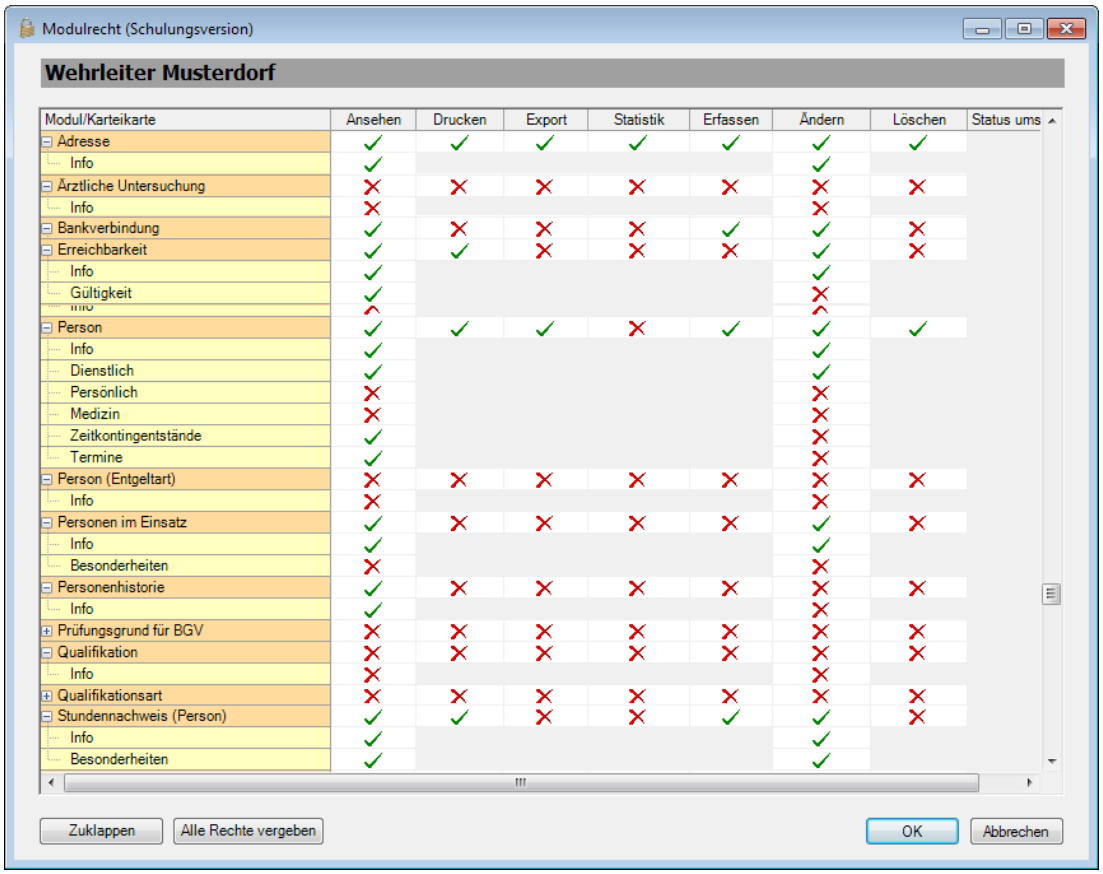
- Modulrechte
- Datengruppenrechte
- Sonderrechte

Die aktuell versorgten Modulrechte der Benutzerprofile können über die Report-Funktion in ARIGON® PLUS ausgedruckt werden.

2.3.1 Modulrechte

Modulrechte erlauben, pro Benutzerprofil dedizierte Rechte in bzw. auf Module (Fenster der Programmmodule) zu definieren. Dies umfasst Berechtigungen zum Ansehen, Bearbeiten, Löschen, Drucken, Export, Statistiken, Status umsetzen (Steuerung von elektronischen Einrichtungen). Die Module sind thematisch unterteilt, so dass bspw. ein Benutzer zwar die Telefonnummern einsehen kann, nicht jedoch ärztliche Untersuchungen.

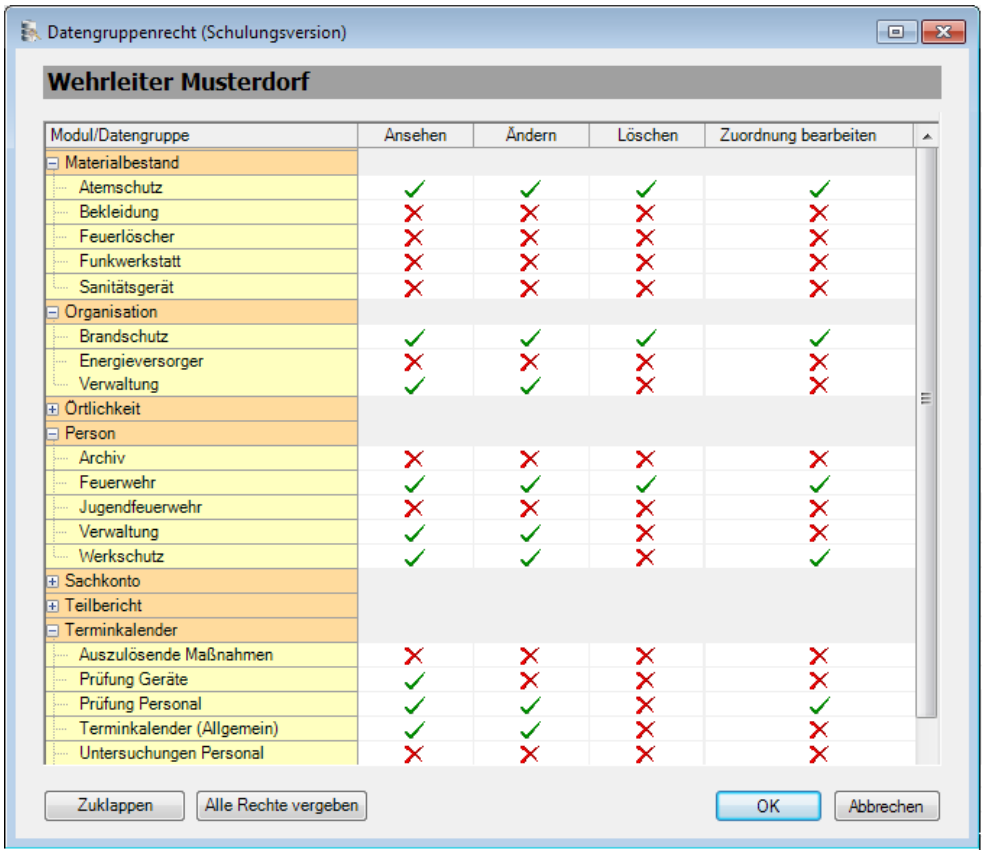
Darüber hinaus ermöglicht ARIGON® PLUS für jede Karteikarte innerhalb eines Moduls separat die Rechte zu konfigurieren. Für jede Karteikarte kann einzeln der Zugriff eines Benutzers zugelassen bzw. gesperrt werden. Die Karteikarten sind thematisch unterteilt, so dass bspw. ein Benutzer zwar die dienstlichen Daten einsehen kann, nicht jedoch besonders schützenswerte Infos wie bspw. Geburtsdatum oder Familienstand.



2.3.2 Datengruppenrechte

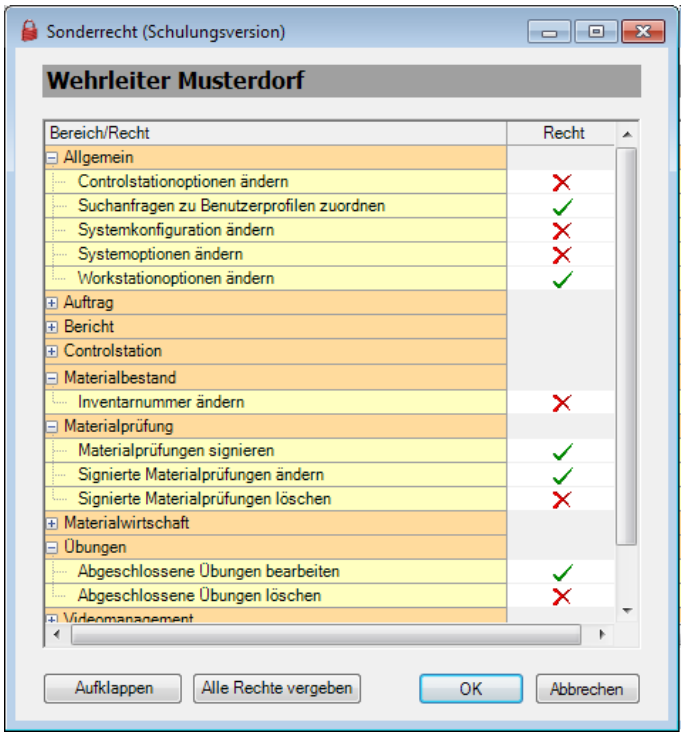
Datengruppenrechte stehen in bestimmten Bereichen zur Verfügung. Sie regeln die Zugriffe auf einzelne Datensätze innerhalb eines Moduls. Datengruppenrechte sind eine weitere Rechteebene. Mit den Datengruppenrechten kann eine zusätzliche Unterscheidung der Daten innerhalb eines Moduls getroffen werden. Jeder Datensatz kann ein oder mehreren Datengruppen zugeordnet werden. Dies ermöglicht Personendaten in solche Datengruppen zu unterteilen. Jede Datengruppe kann für den Zugriff eines oder mehrerer Benutzer zugelassen bzw. gesperrt werden.

Beispielsweise kann so eine Trennung zwischen den Berechtigungen der Atemschutzwerkstatt (nur Bearbeitung der Geräte des Atemschutzes) und der Funkwerkstatt (nur Bearbeitung der Melder und sonstiger funktechnischer Geräte) hergestellt werden. Ebenso kann ein Benutzer Informationen zu Personen seiner eigenen Abteilung verwenden, nicht jedoch Personendaten aus anderen Abteilungen.



2.3.3 Sonderrechte

In ARIGON® PLUS können Sonderrechte vergeben werden. Sonderrechte werden systemseitig angeboten, wenn eine feingranularere Rechtesteuerung benötigt wird, die über die Modul- und Datengruppenrechte nicht abdeckbar sind.



2.3.4 Weitere Rechteverwaltung

Neben obigen allgemeinen Rechteverwaltungen gibt es im Bereich Dienstplan/Wachbuch weiterhin die Möglichkeit, Anseh- und Bearbeitungsrechte auf die Planung zu regeln.

3 Löschkonzepte

Das Kapitel Löschkonzepte gliedert entsprechend der Konzepte, die in den unterschiedlichen Modulen Anwendung finden. Hierbei wurde größte Sorgfalt darauf gelegt, alle Vorkommnisse von Erfassungen personenbezogener Daten aufzuführen.

3.1 Modul Person

Im Modul Person können Datensätze manuell gelöscht werden. Eine automatisierte Löschung ist nicht vorgesehen, da automatisiert das Risiko der Falschlöschung zu groß ist. Bei einem manuellen Löschvorgang werden nachfolgend beschriebene Regeln angewendet.

Beim Löschen einer Person werden verknüpfte Daten in den folgenden Modulen mitgelöscht:

- Adresse
- Ärztliche Untersuchung
- Bankverbindung
- Bekleidungsgrößen
- E-Mail-Empfängergruppe (Erreichbarkeiten)
- Fortbildung
- KatS-Helfer
- Notiz
- Personenhistorie
- Schaltauftrag (Benachrichtigungen)
- Qualifikation
- Zeitkontingentnutzung
- Merkmal (Person)
    - das Merkmal selbst bleibt erhalten
- Objekt (Person)
    - das Objekt selbst bleibt erhalten
- Person (Entgeltart)
    - die Entgeltart selbst bleibt erhalten
- Teilnehmer (Fortbildungsplanung)
    - die Fortbildungsplanung selbst bleibt erhalten
- Zuordnung Datengruppe zu Person
    - die Datengruppe selbst bleibt erhalten
- Zuordnung Leistungsverzeichnis zu Bericht
    - der Bericht und das Leistungsverzeichnis selbst bleiben erhalten
- Zuordnung Person zu Kategorie Person
    - die Kategorie selbst bleibt erhalten
- Zuordnung Person zu Organisation
    - die Organisation, die Abteilung und der Abteilungsbereich selbst bleiben erhalten
- Zuordnung Person zu Sachgebiet
    - das Sachgebiet selbst bleibt erhalten

- Erreichbarkeit
    - wenn eine Alarm-Kurzwahl, Telefon-Kurzwahl oder Geplante Aktion definiert ist, ist das Löschen der Person nicht möglich; siehe nachfolgende Regel
- Lagerort
    - wenn noch Material auf dem Lagerort lagert, ist das Löschen der Person nicht möglich; siehe nachfolgende Regel
- Stundennachweis (Person)
    - zu Stundennachweisen gehörende „Entgelt (Einzelpositionen)“ werden mitgelöscht

Um Datenfragmente zu vermeiden ist das Löschen einer Person nicht möglich, wenn sie in den folgenden Modulen zugehörige Daten besitzt:

- Einsatzmittel
- KatS-Plan Zeile
- Erreichbarkeit, sofern Alarm-Kurzwahl, Telefon-Kurzwahl oder Geplante Aktion definiert ist
- Lagerort, sofern noch Material auf dem Lagerort lagert

Für an Personendatensätze angehängte Dokumente gilt:

Per Option kann geregelt werden, ob

(a) Dokumente generell mitgelöscht werden sollen oder

(b) Dokumente generell nicht mitgelöscht werden sollen oder

(c) der löschende Benutzer gefragt werden soll.

Falls mit gelöschten Personen verknüpfte Dokumente aufgrund der Konfiguration oder aufgrund der Entscheidung eines Benutzers nicht gelöscht wurden, können diese nachträglich manuell gelöscht werden.

3.2 Modul Ereignismanagement

Es wird davon ausgegangen, dass Einsätze in ARIGON® PLUS mit Abschluss des realen Einsatzes ebenso im System abgeschlossen werden. Demnach werden alle Personenbezogenen Daten, die in Verbindung von Einsätzen erfasst werden (Einsatzmittel, Meldender, Besatzung, …), im Löschkonzept für Modul Einsatzdokument behandelt.

3.3 Modul Einsatzdokument

Um regionalspezifische bzw. unternehmensspezifische Aufbewahrungsfristen einzuhalten sowie die Daten für etwaige Untersuchungen zu sichern, ist für Einsatzdokumente eine manuelle Löschung unter Sonderrecht vorgesehen. Mit dem Sonderrecht zum Löschen von Einsatzdokumenten können die Einsatzdokumente inkl. aller daran hängender Daten manuell gelöscht werden.

3.4 Module mit Feldern für personenbezogene Daten

In manchen Modulen sind anforderungsbedingt einzelne Felder integriert, die expliziten Bezug auf Personendaten besitzen; beispielsweise das Feld „Teilnehmer“. Diese Einträge sind nicht an Datensätze aus dem Modul Person gebunden und müssen gesondert behandelt werden. Die Entkopplung

zum Modul Person kann sich beispielsweise aus der Anforderung Archivcharakter ergeben, so dass die Eingaben bzw. der Datenbestand zum Zeitpunkt des Befüllens des Feldes aufgezeigt werden soll. Für Felder mit potentiell Personenbezogenen Daten in den nachfolgend aufgelisteten Modulen ist demnach ein manueller Löschvorgang vorgesehen:

- Baugenehmigungsverfahren
- Berichte
    - Kostenträger-Bericht
    - Abrechnung-Bericht
- Buchung
- Dienstplan
- Fahrtenbuch
- Kurzadressen
- Lagedokumentation
- Schlüssel
- Termin
- Übungen
- Vorbeugender Brandschutz
- Wachbuch
- *einzeln oder über zugeordnetem/r Bericht/Abrechnung/Abrechnung Auftrag löschbar:*
    - Arbeitgeber
    - Patient
    - Personen
    - Kostenträger
    - Kunden
    - Versicherte
- *einzeln oder über zugeordneter Übung löschbar:*
    - Übungsteilnehmer
- Alle Prüfungsmodule bzw. Historienmodule

3.5 Protokolle bzw. Protokollierungseinträge

3.5.1 Controlstationprotokoll und Meldungsfensterprotokoll

Über das Modul „Controlstationprotokoll“ kann dieses Protokoll manuell gelöscht werden, sofern Controlstation lizensiert ist.

Per Option „System / Controlstation / Allgemein / Controlstationprotokolle löschen, die älter als X Tage sind“ ist ein automatisches Löschen einstellbar.

3.5.2 Steuer- und Messpunktprotokoll

Per Option „System / Automatisches Löschen/Automatische Archivierung / Steuer- und Messpunkt-protokoll: Aktion“ ist konfigurierbar, ob nicht gelöscht, gelöscht oder archiviert werden soll.

Per Option „System / Automatisches Löschen/Automatische Archivierung / Steuer- und Messpunkt-protokoll: Mindestalter für Aktion“ ist konfigurierbar, wie lange die Einträge mindestens in ARIGON® PLUS zu halten sind, bevor sie gelöscht /archiviert werden dürfen.

3.5.3 Schaltauftragsprotokoll

Per Option „System / Schaltauftrag / Protokoll / Schaltauftragsprotokolle, die älter als X Tage sind, automatisch löschen (0 = nie löschen)“ ist ein automatisches Löschen einstellbar.

3.5.4 Benutzerprotokoll

Per Option „System / Benutzerprotokoll / Benutzerprotokoll aktivieren“ kann das Anlegen von Benutzerprotokoll komplett verhindert werden.

Per Option „System / Automatisches Löschen/Automatische Archivierung / Benutzerprotokoll: Aktion“ ist konfigurierbar, ob nicht gelöscht, gelöscht oder archiviert werden soll.

Per Option „System / Automatisches Löschen/Automatische Archivierung / Benutzerprotokoll: Mindestalter für Aktion“ ist konfigurierbar, wie lange die Einträge mindestens in ARIGON® PLUS zu halten sind, bevor sie gelöscht /archiviert werden dürfen.

3.5.5 Szenarien-Viewer

Per Option „System / Szenarien / Automatisches Löschen von ‚veralteten‘ Szenarien nach x Tagen (0-nicht löschen)“ ist ein automatisches Löschen für nicht abgeschlossene Szenarien einstellbar.

Per Option „System / Szenarien / Automatisches Löschen von abgeschlossenen Szenarien nach x Tagen (0-nicht löschen)“ ist ein automatisches Löschen abgeschlossener Szenarien einstellbar.

Die Protokolle der über die obigen Optionen gelöschten Szenarien werden bei Löschung des Szenarios mitgelöscht.

3.5.6 Kurzzeitdoku

Da die Kurzzeitdoku an den Arbeitplatz gebunden ist, gibt es hier eine Arbeitsplatz-abhängige Option: „Workstation / <Arbeitplatz> / Controlstation / Kurzzeitdokumentation / Maximales Alter für Aufnahmen in Tagen (0 = nicht löschen)“. Die betreffenden Einträge werden nach Ablauf automatisch gelöscht.

3.5.7 GMA-Protokoll

Per Option „System / Automatisches Löschen/Automatische Archivierung / GMA-Protokoll: Aktion“ ist konfigurierbar, ob nicht gelöscht, gelöscht oder archiviert werden soll.

Per Option „System / Automatisches Löschen/Automatische Archivierung / GMA-Protokoll: Mindestalter für Aktion“ ist konfigurierbar, wie lange die Einträge mindestens in ARIGON® PLUS zu halten sind, bevor sie gelöscht /archiviert werden dürfen.

3.5.8 Protokollierungen

In manchen Modulen kann darüber hinaus trotz Löschung eines Personendatensatzes ein Protokolleintrag bestehen bleiben, der Personenbezogene Daten enthält. Dies ist z.B. gegeben, wenn ein Lagerort aus einer Person erstellt wurde, demnach der Bezeichner des Lagerorts aus Personendaten besteht. Wird die Person gelöscht, wird implizit der Lagerort gelöscht, jedoch nicht dessen Protokolleinträge. Diese sind manuell zu löschen.

Dies gilt für die Module

- Inventureintrag
- Materialbestände
- Materialbuchung (Protokoll)
- Wareneingangsprüfungen

Für Protokolleinträge im Material verhält es sich ähnlich, hierbei kann jedoch eingestellt werden ob die Protokolleinträge 1. mitgelöscht werden sollen, 2. nicht gelöscht werden sollen oder 3. der Benutzer gefragt werden soll. Im Falle von 2. nicht löschen bzw. wählt der Benutzer bei 3. nicht löschen, können die Einträge manuell gelöscht werden.

3.6 Datensatz-Metadaten

Für jeden Datensatz hinterlegt das System Benutzerkürzel und Zeitpunkt für das Erstellen sowie das Ändern eines Datensatzes. Diese Metadaten bleiben am Datensatz bestehen, bis der Datensatz erneut verändert wird (aktueller Bearbeiter wird hinterlegt) oder bis der Datensatz gelöscht wird. Die Metadaten können nicht entfernt werden.

3.7 Datenexporte

Datenexporte liegen im Zuständigkeitsbereich des Lizenznehmers und können aufgrund fehlender Zugriffs- und Verwaltungsmöglichkeiten nicht durch ARIGON® PLUS behandelt werden. Dies gilt insbesondere für

- Externer Datentransfer
- Interner Datentransfer
- Archivdateien (z.B. VdS3534-Protokoll, Steuer- und Messpunktprotokoll, Benutzerprotokoll)

3.8 Fehlerprotokolle

ARIGON® PLUS kann Laufzeitprotokolle zur Ablauf- und Fehleranalyse erstellen. Je nach Einstellung kann nicht ausgeschlossen werden, dass Personenbezogene Daten in diese Fehlerprotokolle abgelegt werden.

Fehlerprotokolle werden standardmäßig im Rolling-File-Verfahren erstellt und überschrieben. Das bedeutet, neuere Einträge überschreiten und vernichten ältere Einträge, sofern das Kontingent verfügbarer Fehlerprotokoll-Zeilen überschritten wird. Das Kontingent sowie die Protokollsensibilität können (mit entsprechenden Betriebssystem-Zugriffsrechten) konfiguriert werden.

