Datenschutzverordnung der EU (DSGVO) Auswirkungen auf Neodat

Bei Neodat handelt es sich um primär um eine Qualitätssicherungssoftware zur Erhebung der Daten für die Neonatalerhebung und NeoKISS.
Je nach Anwendung kann Neodat gleichzeitig zur Schreibung der Arztbriefe, der Erfassung der DRG-Daten, der Erfassung der Stationsbelegung und -besetzung laut gBA /QFR-RL9 u.a. genutzt werden. Dafür müssen natürlich weitere Daten zum Verlauf usw. erfasst werden.

Die Daten werden in elektronischer Form (derzeit XML) an die Erhebungszentren für die Neonatalerhebung und NeoKISS in anonymisierter Form gemeldet.
Seit 2018 beinhaltet die Neonatalerhebung auch personenidentifizierende Daten (PID).
Diese Daten werden entsprechend der Spezifikation der Neonatalerhebung vor der Übermittlung per Email zweistufig verschlüsselt (1. Asymmetrische Verschlüsselung der PID und QS-Daten mit zwei unterschiedlichen öffentlichen Schlüsseln im XML-Dokument, 2 symmetrische Transportverschlüsselung des XML-Dokumentsmit AES).
Die PID können nur von der zentralen Vertrauensstelle entschlüsselt werden, die diese in pseudonymisierter Form dann weitergibt.

Neodat speichert nur Sekundärdaten, die in anderer Form (papiergestützt, KIS, PDMS) auch in anderen Systemen vorliegen.
Die Informationspflicht der betroffen Person ist damit von der allgemeinen Information zur Speicherung personenbezogener Daten im Rahmen des Aufnahmeprozesses im Krankenhaus mit abgedeckt

Die gespeicherten Daten lassen sich in Form des generierten Arztbriefes (Doc/PDF) und Form des Erhebungsbogens der Neonatalerhebung jederzeit auf Anfrage ausgeben.
Eine Ausgabe des gesamten Datensatzes als XML-Daten wäre auch möglich, erscheint aber neben den beiden anderen Ausgabemöglichkeiten wenig sinnvoll, da sich kein zusätzlicher Informationsgewinn ergibt.

Speicherfristen:

Nach Ablauf der Speicherfristen von 10 bzw. ggf. 30 Jahren lassen sich die Daten löschen bzw. ggf. anonymisieren.
Dabei werden die Datensätze vor einem wählbaren Aufnahmedatum gelöscht oder es werden die personenbezogenen Informationen wie Fall- und Patientennummer, Namen, Versicherungsdaten, generierte Dokumente mit anonymen generischen Werten überschrieben, entfernt oder gelöscht.

Umsetzung der Betroffenenrechte:

1. Auskunftserteilung
   Auf Anfrage des Patienten können die erfassten Daten jederzeit in Form des generierten Arztbriefes und des Bogens der Neonatalerhebung als Ausdruck oder als Doc- bzw. PDF-Datei ausgegeben werden.
2. Übertragbarkeit der Daten
   Siehe bei Punkt 1.
   Die Daten der Neonatalerhebung lassen sich zusätzlich auch für einen einzelnen Patienten im XML-Format laut Spezifikation des IQTIG ausgeben.
3. Selektive Einschränkung der Datenverarbeitung
   Da es eine gesetzliche Pflicht zur Erfassung der QS-Daten der Neonatalerhebung gibt, lässt sich für jeden Patienten individuell einstellen, ob nur die gesetzlich vorgeschriebenen Daten oder darüber hinaus auch die Daten für den Arztbrief erfasst werden sollen.
4. Recht auf Berichtigung
   Fehlerhafte Daten lassen sich problemlos korrigieren
5. Löschung von Datensätzen „Recht auf Vergessen“
   Neodat bietet die Möglichkeit einzelne Datensätze (Fälle oder auch Patient mit all seinen Fällen) zum Löschen zu markieren. Sie werden dann nicht mehr angezeigt.
   Beim einem Datenbankintegritätstest mit Datenbankkomprimierung werden die Daten dann auch physikalisch aus der Datenbank entfernt.

Schutz vor Datenverlust

Durch technisch geeignete Verfahren muss der Betreiber von Neodat (zum Beispiel durch regelmäßige Backups) dafür sorgen, dass im Falle eines Datenverlustes durch Hardwarefunktionsstörungen (z.B. Festplattencrash) oder durch Datenkorruption (z.B. durch Rechnerabsturz, Netzprobleme oder ähnliches) sich die Daten zeitnah ohne relevanten Datenverlust wiederherstellen lassen.

Schutz vor unrechtmäßiger Verarbeitung und unberechtigtem Zugriff

Neodat ist mit einem differenzierten Zugriffsrechtekonzept ausgestattet. Auf dieser Grundlage sind die Zugriffsrechte der einzelnen Nutzer klar bestimmt.
Der Nutzer bekommt jeweils nur die für Ihn freigegebenen Funktionen angezeigt.

Eine Schwachstelle des seit vielen Jahren bestehenden Systems liegt systembedingt in der Datenbank.
Da es sich nicht um ein Client-Server-System, sondern um eine filebasierte Datenbank handelt, muss der Nutzer von Neodat direkten Zugriff auf die Datenbankfiles haben. Es ist also theoretisch ein direkter Zugriff auf die Datenbankdateien außerhalb der Applikation möglich.
Unter den Bedingungen eines Medizinischen Netzwerks (nach DIN EN 80000-1 und Technical Reports TR 80001-2-X) , einer entsprechenden Rechtevergabe beim Dateizugriff und der Verschlüsselung der Daten durch das Betriebssystem (EFS) ist bei bestimmungsgemäßen Gebrauch von keiner inadäquaten Datenschutzgefährdung auszugehen.

Um die Sicherheit bezüglich des ungewollten akzidentellen aber auch unberechtigten Datenzugriffs zu verbessern, muss auf die Zugriffssteuerung des Dateisystems zurückgegriffen werden.
Es bieten sich mehrere Möglichkeiten an:

1. Expliziter Start in eine Terminalserversession ohne Zugriff auf Betriebssystemebene

2. Verhinderung des direkten Datenzugriffs über gesperrte Directory-Ebene
   Verzeichnisbaum: Basisdirectory_bzw_share\gesperrtesVerzeichnis\komplexerName\neodat
   a. Das „gesperrte Verzeichnis“ ist (nur auf dieser Ebene) für den Zugriff durch Neodat-Nutzer gesperrt, sie haben in dieser Verzeichnisebene also keinen Zugriff und können über den Explorer oder vergleichbare Programme auch die darunterliegenden Verzeichnisse nicht anzeigen.
   b. Die nächste Ebene hat dann einen komplexen Namen mit Zugriffsrechten für Neodat-Nutzer.
   c. Darunter liegen die eigentlichen Datendirectories.

   Auf die Neodat-Daten kann dann nur mit Wissen des Directory-Namens direkt zugegriffen werden, da im Explorer und vergleichbaren Programmen der Inhalt der gesperrten Verzeichnisebene nicht angezeigt werden kann.
   Wenn dieser Name ausreichend komplex gewählt wird, ist damit eine vergleichbare Sicherheit wie mit einem Passwort zu erreichen.

   Der Pfad wird verschlüsselt (muss in der Neodat-Konfiguration eingeschaltet werden!) in der Neodat-Konfiguration gespeichert und kann damit auch dort nur von Neodat gelesen werden.
   Eine Einsicht und Änderung des Pfades ist nur in Neodat selbst mit Administratorrechten möglich.

3. Start mit **runas** (ggf. mit /savecred) (oder besser Alternativen z.B. RunApp https://www.horland.de/runas.html) und speziellem User mit Zugriff auf Datenbankfiles)

4. Impersonation durch Neodat
   Diese Methode meldet Neodat in eigenem Benutzerkontext mit Zugriff auf die Datenbank an. Sie funktioniert meines Wissens aber nur mit Windows Servern und nicht mit anderen Serverbetriebssystemen.
   Zusätzlich sind u.U. noch Registry-Einstellungen am Server zu machen

Am einfachsten ist sicherlich die Methode 2 zu implementieren, die im oben genannten Netzwerkkontext eine ausreichende Datensicherheit für die in Neodat erfassten Daten bietet.

Als weitere Erhöhung der Sicherheit lässt sich jetzt in der Konfiguration auch die Notwendigkeit der Eingabe eines sichereren Passwortes einstellen.

- case sensitiv
- mindestens 8 Zeichen
- mindestens ein Großbuchstabe
- mindestens eine Ziffer
- mindestens ein Sonderzeichen

Das Passwort wird nicht im Programm gespeichert, sondern nur ein Salted Hash-Wert