Datenschutzverstoß secunet-Konnektor

Bezug: c't-Artikel mit dem Titel „DSGVO-Zwickmühle“ in Ausgabe 6/2022, S. 36.

- secunet-Konnektor mit aktueller Firmware 4.10.1 speichert die ICCSN der eGK in Konnektor-Logs. Es wird allerdings nicht klar gesagt in welchem Log: VSDM-Fachmodul-Log, was gemäß Anforderung Nr. TIP1-A_4710[1)] aus der Konnektorspezifikation[2)] und erlaubt wäre, oder Security-Log, was gemäß der Afo nicht erlaubt wäre.
- Die ICCSN lässt sich (nur) vom TSP (VDA) auflösen. Eine (illegale!) Zusammenführung der TSP-Daten mit den Logs des Konnektors könnte also offenbaren, welcher Patient zu welchem Arzt geht.
- c't hat dies Mitte Januar dem BfDI gemeldet, wobei der genaue Wortlaut der Meldung nicht veröffentlicht ist.
- Der BfDI stellte laut c't „eine Datenschutzverletzung nach Art. 33 Abs. 1 DSGVO“ fest, wobei auch der genaue Wortlaut der Antwort des BfDI nicht veröffentlicht ist.
- Zudem antwortet der BfDI auf die Frage, wer für den konstatierten Datenschutzverstoß verantwortlich sei: „Datenschutzrechtlich verantwortlich für die Konnektoren sind diejenigen, die diese für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen, sowie sie über die Mittel der Datenverarbeitung mitentscheiden.“ In dieser Allgemeinheit nur eine Paraphrase der Zuweisung der datenschutzrechtlichen Verantwortlichkeiten, wie sie § 307 SGB V Abs. 1 S. 1 regelt. Gemeint sind damit (so auch die Antwort des BfDI auf explizite Nachfrage der c't) die Ärzte und Leistungserbringer.

In einer Stellungnahme erklärt secunet die technischen Hintergründe der ICCSN-Speicherung. Gleichzeitig wird behauptet, bei den ICCSN handele es sich nicht um personenbezogene Daten und man verstoße weder gegen die Spezifikation noch gegen den Datenschutz.

Auch die gematik ordnet das Thema nochmals in einer News ein. Dort wird explizit von nicht spezifikationskonformen Verhalten gesprochen.

Verschiedene Artikel in der Fachpresse greifen das Thema auf.

Die KBV wendet sich per Schreiben an die gematik und fordert Aufklärung. Sie sieht die gematik in der Verantwortung, da diese den secunet-Konnektor zugelassen habe, obwohl er gegen Datenschutzanforderungen der gematik-Spezifikationen verstoße.

Weitere Artikel, die das Thema auf Basis des c't-Artkels aufgreifen:

- Negt, Alexandra. IT-Experten schlagen Alarm: Konnektoren speichern Praxisdaten, apotheke ad-hoc, 26.2.2022.
- Urbanek, Margarethe. DSGVO-Verstöße bei Konnektoren: Ärzte in der Verantwortung? ÄrzteZeitung online, 25.2.2022. (hinter Paywall)
- Datenverstöße aufgedeckt: Neuer Ärger um TI-Konnektoren, aerzteblatt.de, 25.02.2022

Reaktion der KBV:

- KBV fordert unverzügliche Aufklärung des Sicherheitsvorfalls in der TI – Verantwortung liegt bei der gematik, Praxisnachrichten 25.2.2022.

Reaktion des BMG

- BMG legt in einem Schreiben dar (Schreiben liegt mir vor), dass Ärzt:innen nicht verantwortlich seien für den Vorfall. Allerdings zitiert das BMG das Gesetz hier falsch.[3] Es ist nirgendwo eindeutig gesagt, in welchem Log die ICCSN nun gespeichert wird, aber die gematik meldet Spezifikationsverstoß, es handelt sich also wohl nicht um das VSDM-Protokoll. Hat die gematik als zulassende Instanz recht, stimmt die Behauptung in der secunet-Stellungnahme nicht. Wenn die ICCSN - und damit wohl personenbezogene Daten - außerhalb des VSDM-Fachmodul-Log gespeichert werden, wird gegen eine Datenschutzanforderung verstoßen. Die gematik hat somit einen Konnektor zugelassen, der nicht konform ist zu dieser Datenschutzanforderung. Ärzt:innen müssen Konnektoren laut gesetzlicher Vorgabe nutzen. Der BfDI - zumindest laut c't - sieht einen datenschutzrechtlichen Verstoß gegen Art. 33 Abs. 1 DSGVO. In diesem Artikel geht es eigentlich aber um die **Meldung** einer Datenschutzverletzung, nicht um die unzulässige Verarbeitung personenbezogener Daten ohne hinreichende Gesetzesgrundlage bzw. entgegen der Spezifikationsvorgabe der gematik. Ein Verstoß gegen Art. 33 wäre die fehlende **Meldung** des Vorgangs bei Bekanntwerden. Wie sollen Ärzt:innen etwas melden, von dem sie (noch gar) nichts wissen? Meldung müsste zudem nur erfolgen, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“. Ein Risiko bestünde nur, wenn der Ärzt:innen die Logs - illegalerweise(!) - an einen TSP geben würden.[4] Hier fehlt aus meiner Sicht eine klare Stellungnahme des BfDI zu dem Thema, das immerhin über 100.000 Ärzt:innen und deren Patient:innen betrifft! Mindestens könnte man erwarten, dass die c't den genauen Schriftverkehr mit dem BfDI zur Klärung offenlegt. Ein Zugriff der TSP auf die Logs ist ohne Herausgabe der Logs nicht möglich. Wenn nun der datenschutzrechtlicher Verstoß im Sinne unzulässiger Verarbeitung personenbezogener Daten vorläge, wären Ärzt:innen gemäß der eigenartigen Gesetzeslage des § 307 SGB V verantwortlich für etwas, von dem sie in der Regel nicht mal wissen, dass es existiert. Welche Ärzt:innen wissen, dass es eine ICCSN gibt, was das ist und dass sie in einem Log (was ist das?) ihres Konnektors (was war das nochmal genau?) gespeichert wird. Hier liegt das eigentliche Problem und der Aufreger, dass bspw. auch im ersten Teil einer Artikel-Serie zum PDSG vom Juristen Carsten Dochow detailliert beleuchtet wird.

1)

Der Konnektor DARF medizinische Daten NICHT in die Protokolldateien schreiben.
Personenbezogene Daten DÜRFEN NICHT in Protokolleinträgen gespeichert werden.
KVNR, ICCSN und CardHolderName MÜSSEN als personenbezogene Daten behandelt werden.
Die ICCSN DARF Im Fehlerfall durch Fachmodule in Protokolleinträgen gespeichert werden. Die ICCSN DARF NICHT im Sicherheitsprotokoll gespeichert werden.

2)

Version 4.11.1 und Version 5.8.0

3)

Praxen sind nicht für Fehler von Konnektoren verantwortlich - BMG bestätigt KBV-Auffassung zum Datenschutz, KBV-Praxisnachrichten vom 1.3.2022)

Meine Bewertung

- ICCSN ist ein persönliches Datum, da sie prinzipiell auf persönliche Daten zurückzuführen ist. Gemäß „absoluter“ Auslegung der DSGVO diesbez. gelten solche (prinzipiell auflösbaren) Daten als personenbezogen. 100% eindeutig ist das rechtlich aber wohl nicht, da durchaus auch die „relative“ Auffassung vertreten wird, dass nur als personenbezogen gilt, was der datenschutzrechtlich Verantwortliche auch selbst zuordnen kann oder im Rahmen bspw. einer Auftragsverarbeitung auflösen lassen könnte. Die absolute Auffassung widerspricht somit der secunet-Stellungnahme. Konsequenterweise fordert auch die relevante Anforderung TIP1-A_4710: „KVNR, ICCSN und CardHolderName MÜSSEN als personenbezogene Daten behandelt

werden.“ Einzige Ausnahme ist das Fachmodulprotokoll.((„Die ICCSN DARF Im Fehlerfall durch Fachmodule in Protokolleinträgen gespeichert werden. Die ICCSN DARF NICHT im Sicherheitsprotokoll gespeichert werden.“

[4)]

Diese Argumentation taugt m.E. allerdings nichs gegen den grundsätzlichen Datenschutzverstoß der Verarbeitung personenbezogener Daten ohne gesetzliche Grundlage bzw. wider die Spezifikation, da diese ja trotzdem stattfindet unabhängig vom Risiko.