


Hinweise zum Datenschutz beim Betrieb von Alarmierungssystemen

Stand August 2021

Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN

Inhaltsverzeichnis

Allgemeines

Landesweit werden Einsatzkräfte von Feuerwehr, Rettungsdienst, THW und anderen Hilfsorganisationen über Funkmeldeempfänger zu Einsätzen alarmiert. Darauf hatte die Einführung der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 vielfache Auswirkungen. Denn spätestens mit deren Inkrafttreten hatte der Schutz personenbezogener Daten einen nochmals gesteigerten Stellenwert erhalten.

Seither wurden in den Integrierten Leitstellen Prozesse überprüft, und vielfältige Schutzmaßnahmen zur Gewährleistung der Sicherheitsanforderungen an den Umgang mit personenbezogenen Daten ergriffen. Dies erfolgte gerade auch in Hinblick auf die verschiedenen Abläufe, und auf den Betrieb der in den Stadt- und Landkreisen betriebenen Alarmierungsnetze. In vielen Leitstellenbereichen mussten zusätzliche Vorkehrungen für eine datenschutzkonforme Abwicklung der Alarmierung der Einsatzkräfte getroffen werden. Nach Artikel 32 DSGVO müssen die verantwortlichen Stellen dazu technische und/oder organisatorische Maßnahmen ergreifen. In der Praxis ergeben sich hier im Wesentlichen zwei Möglichkeiten:

Grundsätzlich sollten alle Komponenten des Systems (vom Leitrechner bis zum Meldeempfänger) eine Verschlüsselung der übertragenen Daten zulassen, die Alarmmeldungen sollten **Ende-zu-Ende-verschlüsselt** übertragen werden.

Wo das Alarmierungssystem eine solche technische Umsetzung des Schutzes der personenbezogenen Daten nicht gewährleisten kann, müssen organisatorische Maßnahmen getroffen werden. In der Regel kommt hier als einzige Möglichkeit in Betracht, **ausschließlich Daten ohne Personenbezug** zu übermitteln; also maximal Alarmort, -art und Straße, keinesfalls jedoch Hausnummern, Namen oder gar Patientendaten wie Diagnosen oder Vorerkrankungen.

Mancherorts hat sich neben den primären Alarmierungssystemen die Benachrichtigung auf Smartphones oder sonstigen IT-Geräten via SMS, Push-App oder E-Mail etabliert. So können beispielsweise Einsatzkräfte an Arbeitsorten erreicht werden, die außerhalb des Alarmierungsnetzes liegen. Auch Anzeigetableaus und Steuerungssysteme für die Gebäudetechnik in Feuerwehrhäusern, Feuerwachen und Unterkünften werden angesteuert. So vielfältig die Gründe für den Einsatz solcher Systeme sind: Für sie gelten **die gleichen Anforderungen an den Datenschutz, wie für die primären Alarmierungssysteme**. Nachfolgend wird ein Überblick über die Technik, die zu beachtenden Vorgaben und über die Konsequenzen bei Nicht-Beachtung gegeben.

Funktionsweise

Die digitale Alarmierung über Funkmeldeempfänger erfolgt im POCSAG-Standard auf speziell für berechtigte Nutzer der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zugewiesenen Funkfrequenzen. In modernen Alarmierungsnetzen besteht die Möglichkeit, die übertragenen Daten zu verschlüsseln. Die Alarmierungsdaten sind dadurch auf dem Übertragungsweg grundsätzlich vor unbefugtem Zugriff geschützt.

Erfolgt die Übertragung im Alarmierungsnetz unverschlüsselt, so können die Daten mittels eines Funkscanners oder über die serielle Schnittstelle an der Ladeschale eines Digitalen Meldeempfängers (DME) und mithilfe frei erhältlicher Software auch durch Unberechtigte abgegriffen und beispielsweise ins Internet übertragen werden. Dieses Vorgehen birgt große datenschutzrechtliche Risiken.

Rechtsgrundlagen

Die bei der Alarmierung übermittelten Daten umfassen regelmäßig sensible Inhalte, wie beispielsweise Informationen zu Einsatzart, -ort und -zeit, sowie Zusatzinformationen zum Geschehen oder zur meldenden Person. Darüber hinaus werden im Rettungsdienst oftmals auch Patientendaten übermittelt. Daher bedarf es rechtlich, wie auch moralisch, eines angemessenen Schutzes dieser personenbezogenen Daten vor Missbrauch und unbefugter Offenlegung.

Bei der Übertragung von Alarmierungsdaten handelt es sich regelmäßig um die **Verarbeitung von personenbezogenen Daten**. Das Datenschutzrecht erlaubt diese Verarbeitung grundsätzlich, da die Verarbeitung der Alarmierungsdaten erforderlich ist, um die den BOS zugewiesenen hoheitlichen Aufgaben erfüllen zu können.

Das Feuerwehrgesetz Baden-Württemberg (FwG) sieht in § 4 Abs. 3 und § 3 Abs. 2 vor, dass die **Land- und Stadtkreise** zur Alarmierung der Gemeindefeuerwehren geeignete Kommunikationsnetze zu errichten und

zu betreiben haben. Da es sich beim Internet nicht um ein „eigenes Netz“ handelt, ist die alleinige Alarmierung auf diesem Weg nicht zulässig. **Allenfalls als Ergänzung**, um Alarmierungen parallel zu übertragen, ist eine Nutzung dieses öffentlichen Netzes vorstellbar.

Betreibt eine kreisangehörige **Gemeinde** ein solches System zur Weiterleitung von Alarmierungsdaten, so entspricht dies folglich nicht der Konzeption des Feuerwehrgesetzes. Datenschutzrechtlich ist der Betrieb dennoch zulässig, soweit er für die Aufgabenerfüllung als erforderlich angesehen werden kann. Dies kommt regelmäßig wohl nur in den eingangs erwähnten Sonderfällen in Betracht.

Datenschutzrechtliche Vorgaben

Dabei müssen auch die weiteren datenschutzrechtlichen Vorgaben eingehalten werden. Seit 2018 stehen personenbezogene Daten unter dem strengen Schutz der europäischen **Datenschutz-Grundverordnung (DSGVO),** welche als unmittelbar anwendbares Recht auch die maßgeblichen Vorgaben für die Datenverarbeitung auf nationaler Ebene trifft.

So erlegt sie den verantwortlichen Stellen beispielsweise umfangreiche Informations- und Dokumentationspflichten auf und verpflichtet sie, weitreichende Rechte von betroffenen Personen (wie die Ansprüche auf Auskunft oder Löschung) zu gewährleisten. Außerdem muss in den meisten Fällen ein Datenschutzbeauftragter benannt werden und ein Verzeichnis über alle Datenverarbeitungsvorgänge erstellt werden (Verarbeitungsverzeichnis).

In Art. 5 regelt die DSGVO die bei der Datenverarbeitung zu beachtenden Grundsätze. Besonders zu beachten ist der sogenannte Grundsatz der **„Integrität und Vertraulichkeit“**. Die Verpflichtung zur Einhaltung dieses Grundsatzes spiegelt sich an vielen Stellen der Verordnung wider (Art. 24, 25, 32 DSGVO), was dessen Wichtigkeit weiter unterstreicht. Im Einklang mit dem nationalen Datenschutzrecht fordert die DSGVO demnach ein **angemessenes Schutzniveau** für personenbezogene Daten vor Missbrauch oder Offenlegung. Was dabei als angemessen anzusehen ist, bestimmt sich nach den Umständen des Einzelfalls. Kurz gesagt ist eine Gesamtabwägung zwischen dem datenschutzmäßigen Risiko und dem Aufwand für entsprechende Schutzvorkehrungen zu treffen. Im Falle der Alarmierungsdaten ist zu berücksichtigen, dass es sich regelmäßig um sehr sensible Daten handelt. Demgegenüber stehen Schutzmaßnahmen, die mit überschaubarem Aufwand genutzt werden können. Insofern kann durchaus ein recht hohes Schutzniveau gefordert werden. Jedenfalls dürfen die Daten **auf keinen Fall offen einsehbar ins Internet gelangen**.

Dies ist jedoch bei einigen Softwarelösungen der Fall, wenn sie nicht entsprechend konfiguriert werden. So ist es beispielsweise im November 2020 gelungen, Einsatzdaten von verschiedenen Feuerwehren frei im Internet einzusehen, die mutmaßlich mittels derartiger Software von einem Funkmeldeempfänger abgegriffen wurden (so berichtet in „c’t“, Heft 23 aus 2020, unter der Rubrik „c’t deckt auf“).

Als weiterer Grundsatz der Datenverarbeitung ist nach der DSGVO der sogenannte Grundsatz der „Datenminimierung“ zu beachten. Das bedeutet, dass personenbezogene Daten nur in dem Umfang und nur solange gespeichert werden dürfen, wie es zur Aufgabenerfüllung erforderlich ist. Diesen Grundsatz gilt es immer zu beachten! Betroffene haben ein Recht auf Löschung ihrer Daten, sobald die Speicherung zur Erfüllung öffentlicher Aufgaben nicht mehr erforderlich ist (Art. 17 DSGVO).

Verantwortung

„Verantwortlicher“ im Sinne der DSGVO ist die Stelle, die maßgeblich über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). Konkret verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben beim Betrieb eines solchen Alarmierungssystems ist also in der Regel die Behörde oder Stelle, welche das System betreibt und somit über Zweck und Mittel der Verarbeitung bestimmt.

Wird der Betrieb an einen externen Dienstleister vergeben, so handelt es sich um eine „Auftragsverarbeitung“ im Sinne von Art. 28 DSGVO. Die **vergebende Stelle haftet dann vorrangig auch für Verstöße seitens des Dienstleisters** (Art. 82 Abs. 2 DSGVO). Außerdem muss ein schriftlicher Vertrag über die Auftragsverarbeitung geschlossen werden, in dem insbesondere Art, Zweck und Ausmaß der Datenverarbeitung geregelt werden müssen.

Umsetzung der Vorgaben

Die DSGVO sowie das nationale Datenschutzrecht verpflichten den Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen (sogenannte TOM) zu treffen, um die Sicherheit und Integrität der Daten zu gewährleisten (Art. 32 DSGVO).

Technische Maßnahmen sind beispielsweise

- Verschlüsselung der Daten entsprechend dem aktuellen Stand der Technik (sowohl bei Übertragung als auch bei Speicherung; bspw. bei Weiterleitung per E-Mail ggfs. unter Einsatz von Ende-zu-Ende-Verschlüsselung mittels S/MIME oder OpenPGP und durch qualifizierte Transportverschlüsselung mittels DANE und DNSSEC bei den beauftragten E-Mail-Providern).
- Passwortschutz beim Zugriff auf die Serverinfrastruktur (ggfs. Zweifaktor-Authentifizierung),
- automatische Protokollierung von Zugriffen (Logdaten), um unbefugte Zugriffe feststellen zu können,
- Begrenzung der gespeicherten Daten auf das erforderliche Minimum: Beispielsweise kann die Datenspeicherung minimiert werden durch die Verwendung von reinen Push-Systemen, bei denen Mitteilungen nicht dauerhaft auf dem Endgerät gespeichert werden; anderenfalls muss eine anderweitige automatisierte Löschung erwogen werden,
- Speicherung auf eigenen Servern oder zumindest nicht bei Drittanbietern,
- Schutz der Datenverarbeitungssysteme vor Angriffen (Firewall/Virenschutz),
- Physischer Schutz der Datenverarbeitungssysteme vor äußeren Einflüssen (z.B. vor Diebstahl, beispielsweise durch Betrieb in einem gesicherten Raum).

Organisatorische Maßnahmen sind beispielsweise

- Einbindung des Datenschutzbeauftragten bei der Einrichtung der Systeme,
- Sensibilisierung und Schulung des Personals im Hinblick auf Schutz und Vertraulichkeit der Daten, z.B. zum sicheren Umgang mit dem Smartphone, sowie auf die möglichen Rechtsfolgen bei Verstößen,
- Begrenzung des Kreises der Zugriffsberechtigten auf das erforderliche Maß,
- regelmäßige Überprüfung von Logdaten auf unbefugte Zugriffe,
- keine Verwendung oder Weitergabe der Daten außerhalb des Erhebungszwecks,
- Bestimmung von Löschfristen, falls keine automatisierte Löschung erfolgen kann; im Hinblick auf die für die Leitstellen geltende Löschfrist (§ 35 Abs. 6 FwG) sollte keine längere Frist als 6 Monate gewählt werden,
- Festlegung eines standardisierten Vorgehens bei Vorfällen oder Verstößen.

Welche der hier aufgeführten Maßnahmen im konkreten Einzelfall praktisch und sinnvoll umsetzbar sind, hängt letztendlich von der verwendeten Technik und den jeweiligen Bedürfnissen ab. Die Aufzählung soll daher nur dazu dienen, einen Eindruck von den gegebenen Möglichkeiten zu verschaffen und erhebt keinen Anspruch auf Vollständigkeit.

Letztendlich gibt es datenschutzrechtlich keine Vorgaben dazu, wie die Schutzmaßnahmen konkret auszusehen haben. Gefordert wird lediglich ein angemessenes Schutzniveau, das dem **aktuellen Stand der Technik** entspricht. Vor diesem Hintergrund sind Verantwortliche dazu aufgefordert, sich mit den gegenwärtig möglichen technischen Maßnahmen auseinanderzusetzen und diese unter Einbeziehung des Implementierungsaufwandes sowie der individuellen Bedürfnisse abzuwägen. Diese Aufgabe muss dynamisch betrachtet werden. Das bedeutet, dass Maßnahmen **in regelmäßigen Abständen auf Aktualität zu überprüfen und gegebenenfalls anzupassen** sind. Dies ist freilich keine alleinige Aufgabe beispielsweise der Feuerwehren als Nutzer. Auch die Träger, im Beispiel einer Feuerwehr die Gemeinde, und deren Datenschutzbeauftragten kommt hier eine bedeutende Funktion zu. Einen Überblick über den aktuellen Stand der Technik sowie geeignete organisatorische Maßnahmen können beispielsweise die „IT-Grundschutz-Bausteine“ des Bundesamts für Sicherheit in der Informationstechnik (BSI – abrufbar unter www.bsi.bund.de) sowie das von den Datenschutzbehörden der Länder und des Bundes entwickelte „Standard-Datenschutzmodell“, (abrufbar unter www.bfdi.bund.de) liefern.

Zuletzt sei noch erwähnt, dass gegebenenfalls das **Verarbeitungsverzeichnis** (Art. 30 DSGVO) um die Verarbeitung der Einsatzdaten ergänzt werden muss. Fer-

ner kann die Durchführung einer **Datenschutzfolgeabschätzung** (Art. 35 DSGVO) vor der Einführung eines entsprechenden Benachrichtigungssystems erforderlich sein.

Rechtsfolgen bei Verstößen und Missbrauch

Der Gesetzgeber misst dem Schutz persönlicher Daten schon seit längerem einen hohen Stellenwert bei. Datenschutzrechtliche Verstöße können daher zu empfindlichen Sanktionen bis hin zur Verwirklichung von Straftaten führen.

Zunächst führen Verstöße gegen Vorgaben der DSGVO dazu, dass die verantwortliche Stelle **für jegliche hierdurch entstandenen materiellen und immateriellen Schäden haftet** (Art. 82 DSGVO). Vor allem angesichts der Tatsache, dass bislang gerichtlich nicht entschieden wurde, welche Positionen unter den Begriff der immateriellen Schäden fallen, besteht ein erhebliches Haftungsrisiko. Außerdem müssen **Datenpannen der zuständigen Aufsichtsbehörde und ggfs. den betroffenen Personen gemeldet werden** (Art. 33, 34 DSGVO).

Greifen einzelne Organisationsangehörige die Alarmierungsdaten eigenmächtig ab, so sind noch schärfere Sanktionen möglich. Dann handelt es sich jedenfalls um eine Ordnungswidrigkeit, die schlimmstenfalls mit einer **Geldbuße** von bis zu 20 Mio. Euro geahndet werden kann (Art. 83 DSGVO).

Darüber hinaus können Verstöße sogar strafrechtlich relevant werden. BOS-Angehörige sind Beamte oder zumindest förmlich Verpflichtete. Sie sind daher Amtsträger oder stehen solchen gleich. Werden Daten offengelegt (beispielsweise indem sie offen einsehbar ins Internet übertragen werden), so kann sich der Verantwortliche wegen der **Verletzung des Privatgeheimnisses (§ 203 StGB)** strafbar machen. Dies kann mit einer Geldstrafe oder einer **Freiheitsstrafe von bis zu einem Jahr** geahndet werden.

In Betracht kommen daneben je nach Einzelfall weitere Amtsträgerdelikte wie die Verletzung des Dienstgeheimnisses (§ 353b StGB), Vorteilsannahme (§ 331 StGB) oder Bestechlichkeit (§ 332 StGB). Die Strafrahmen dieser Delikte reichen bis zu Freiheitsstrafen von 5 Jahren. Als Nebenfolge kann dem Verurteilten zusätzlich die Fähigkeit zur Bekleidung öffentlicher Ämter aberkannt werden. Das hat zur Folge, dass der Betroffene kraft Gesetzes aus dem Feuerwehrdienst ausscheidet (vgl. § 13 Abs. 1 Nr. 6 FwG). Diese Delikte dürften jedoch nur in Extremfällen (beispielsweise beim Verkauf von Alarmierungsdaten) einschlägig sein.

Ebenso strafbar machen können sich Personen, die nicht den BOS angehören. Greifen sie unbefugt Alarmierungsdaten ab, so machen sie sich strafbar wegen des Ausspähens oder Abfangens von Daten (§§ 202a, 202b StGB). Ferner ist das unbefugte Abhören von Funkkommunikation auch nach § 148 Abs. 1 Nr. 1 des Telekommunikationsgesetzes (TKG) strafbar.

Daneben stellen auch die Datenschutzgesetze die unbefugte Verarbeitung von personenbezogenen Daten unter Strafe, wenn sie in der Absicht erfolgt andere zu schädigen oder sich selbst zu bereichern (§ 42 BDSG / § 29 LDSG). Dies kann wiederum auch BOS-Angehörige betreffen, die ohne Zustimmung der Dienststelle Alarmierungsdaten verarbeiten, wenn eine entsprechende Absicht vorliegt. Hier drohen ebenfalls Geldstrafen oder Freiheitsstrafen von bis zu drei Jahren.

Fazit

Die Alarmierung von Einsatzkräften über alternative Alarmierungssysteme, bspw. via Internet auf das Smartphone, stellt eine rechtlich grundsätzlich zulässige Ergänzung zur Alarmierung mittels Funkmeldeempfängern dar. Den umsetzenden Stellen, wie auch den Einsatzkräften, muss jedoch bewusst sein, dass sie hierbei mit sensiblen persönlichen Informationen umgehen. Die personenbezogenen Daten müssen daher angemessen vor Missbrauch geschützt werden. Anderenfalls können empfindliche Folgen bis hin zu Freiheitsstrafen drohen.

Bildnachweis:

Titelseite: Fotolia (links), IM BW (Mitte), Tom Bilger, rechts)