Ministerium des Innern und für Kommunales des Landes Brandenburg

Referat 34

Brand- und Katastrophenschutz, Förderung des Ehrenamtes mit Bezug zum Brand- und Katastrophenschutz, Koordinierungszentrum Krisenmanagement, Zivile Verteidigung, Militärangelegenheiten, Fachaufsicht LSTE, Laufbahnordnungsbehörde feuerwehrtechnischer Dienst

Hinweise zum Datenschutz beim Betrieb von Alarmierungssystemen in der nichtpolizeilichen Gefahrenabwehr im Land Brandenburg

Allgemeines

Landesweit werden Einsatzkräfte von Feuerwehr, Rettungsdienst und Hilfsorganisationen über Funkmeldeempfänger zu Einsätzen alarmiert. Aufgrund der Einführung der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 wurden in den Integrierten Regionalleitstellen 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 Landkreisen und kreisfreien Städten betriebenen Alarmierungsnetze. In vielen Leitstellenbereichen mussten zusätzliche Vorkehrungen für eine datenschutzkonforme Abwicklung der Alarmierung der Einsatzkräfte getroffen werden. 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 Nichtbeachtung 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.

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**. Die Verarbeitung dieser Daten ist zulässig, soweit dies zur Erfüllung der den BOS zugewiesenen hoheitlichen Aufgaben erforderlich ist.

Die Landkreise und kreisfreien Städte betreiben zur Alarmierung der Feuerwehren und des Rettungsdienstes geeignete Kommunikationsnetze. 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. Ob und für welche Daten dies der Fall ist, kann nur nach Auswertung der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) festgestellt werden, bei der die Übermittlung der einzelnen Datenkategorien jeweils zu prüfen ist sowie technische und organisatorische Maßnahmen zur Risikominimierung festzulegen sind.

Datenschutzrechtliche Vorgaben

Bei der Verwendung solcher Systeme 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. Unabhängig davon hatte der erforderliche Schutz der personenbezogenen Daten auch vor dem Inkrafttreten der DSGVO bereits einen hohen Stellenwert.

So erlegt die DSGVO den verantwortlichen Stellen beispielsweise umfangreiche Informations- und Dokumentationspflichten auf und verpflichtet sie, weitreichende Rechte von betroffenen Personen (wie die Ansprüche auf Auskunft oder Löschung, Art. 15 und Art. 17 DSGVO) zu gewährleisten. Außerdem müssen öffentliche Stellen einen Datenschutzbeauftragten benennen (Art. 37 Abs. 1 lit. a DSGVO) und es muss ein Verzeichnis über alle Datenverarbeitungsvorgänge erstellt werden (Verarbeitungsverzeichnis, Art. 30 DSGVO).

In Art. 5 regelt die DSGVO die bei der Datenverarbeitung zu beachtenden Grundsätze. Besonders zu beachten ist der sogenannte Grundsatz der **„Integrität und Vertraulichkeit"** (Art. 5 Abs. 1 lit. f DSGVO). Der Begriff der Integrität betrifft die Unversehrtheit der Daten. Es soll demnach verhindert werden, dass Daten ganz oder teilweise gelöscht, vernichtet oder unbefugt verändert werden. Der Grundsatz der Vertraulichkeit bezieht sich auf den Schutz vor unrechtmäßiger und unbefugter Kenntnisnahme und Verarbeitung. Die Verpflichtung zur Einhaltung der Integrität und Vertraulichkeit spiegelt sich an vielen Stellen der Verordnung wider (Art. 24, 25, 32 DSGVO), was deren Wichtigkeit weiter unterstreicht. Die DSGVO fordert demnach, ggf. ergänzt durch nationale Datenschutzvorschriften, ein **angemessenes Schutzniveau** für personenbezogene Daten vor Missbrauch oder Offenlegung. Was dabei als

angemessen anzusehen ist, bestimmt sich nach den Umständen des Einzelfalls.

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, welches sich ausschließlich am Risiko bemisst, gefordert werden. Erwägungen wie Wirtschaftlichkeit oder die Schwierigkeit der Implementierung können zwar ins Gewicht fallen, wenn sie die Aufgabenerfüllung selbst gefährden, sind aber kein Kriterium bei der Feststellung des erforderlichen Schutzniveaus. Jedenfalls dürfen die Daten **auf keinen Fall offen einsehbar ins Internet gelangen**.

Dies ist jedoch bei einigen Softwarelösungen der Fall, wenn sie nicht ordnungsgemäß 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", S. 26 f.). Dieser Sachverhalt fand auch Berücksichtigung im Tätigkeitsbericht Datenschutz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg zum 31. Dezember 2023 (S. 84 f.).

Als weiterer Grundsatz der Datenverarbeitung ist nach der DSGVO auch der sogenannte Grundsatz der **„Speicherbegrenzung"** (Art. 5 Abs. 1 lit. e DSGVO) und der **„Datenminimierung"** (Art. 5 Abs. 1 lit. c DSGVO) zu beachten. Die Speicherbegrenzung bedeutet, dass personenbezogene Daten nur solange gespeichert werden dürfen, wie es zur Aufgabenerfüllung erforderlich ist. Im Rahmen der Datenminimierung sollte darauf geachtet werden, dass personenbezogene Daten dem Zweck angemessen und auf notwendige Maß beschränkt sein müssen. Das notwendige Maß ist erreicht, wenn der verfolgte Zweck nicht mit weniger Daten erreicht werden kann. Betroffene haben ein Recht auf Löschung ihrer Daten, sobald die Speicherung zur Erfüllung öffentlicher Aufgaben nicht mehr erforderlich ist („Recht auf Vergessenwerden", 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). Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorgaben beim Betrieb eines solchen Alarmierungssystems ist also die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die das System betreibt und somit über Zweck und Mittel der Verarbeitung von personenbezogenen Daten bestimmt. Die Gewährleistung und Umsetzung des Datenschutzes bei der Verarbeitung personenbezogener Daten obliegt daher der Behördenleitung, den Organisationseinheiten und den jeweiligen Beschäftigten bzw. hier den nutzenden Einsatzkräften des Systems. Da die öffentlichen Feuerwehren im Land Brandenburg Bestandteil der öffentlichen Verwaltung sind, sind vor Einrichtung des Systems entsprechend der internen Zuständigkeitsregelungen der örtlichen Aufgabenträger die für die Umsetzung des Datenschutzes zu beteiligenden Stellen der örtlichen Aufgabenträger in Kenntnis zu setzen.

Wird der Betrieb an einen externen Dienstleister vergeben, so handelt es sich um eine „Auftragsverarbeitung" im Sinne von Art. 28 DSGVO. Die vergebende Stelle bleibt dabei datenschutzrechtlich voll verantwortlich und haftet dann vorrangig auch für Verstöße seitens des

Dienstleisters (Art. 82 Abs. 2 DSGVO). Außerdem muss ein Vertrag über die Auftragsverarbeitung geschlossen werden, in dem insbesondere Art, Zweck und Ausmaß der Datenverarbeitung geregelt werden müssen.

Umsetzung der Vorgaben

Die DSGVO sowie ggf. ergänzend 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 (insbesondere 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,
- 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 der IT-Sicherheits- und Datenschutzbeauftragten der örtlichen Aufgabenträger 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) durch
    - verpflichtende Teilnahme an Datenschutzschulungen und Festlegung eines Schulungskonzepts,
    - schriftliche Verpflichtung der Einsatzkräfte auf die Einhaltung des Datenschutzes,
    - Festlegung interner Verhaltensregeln,
    - Merkblätter oder Anleitungen,
- Begrenzung des Kreises der Zugriffsberechtigten auf das erforderliche Maß durch Festlegungen in einem Rechte- und Rollenkonzept,
- regelmäßige Überprüfung von Logdaten auf unbefugte Zugriffe,
- keine Verwendung oder Weitergabe der Daten außerhalb des Erhebungszwecks,

- Bestimmung von Löschfristen in einem Löschkonzept, falls keine automatisierte Löschung erfolgen kann; im Hinblick auf die für die Regionalleitstellen geltende Löschfrist (§ 17 Abs. 3 Satz 2 BbgBKG) sollte keine längere Frist als 6 Monate gewählt werden,
- Festlegung eines standardisierten Vorgehens bei Vorfällen oder Verstößen,
- Festlegung von Maßnahmen zur Gewährleistung und Umsetzung der Betroffenenrechte (Art. 12 ff. DSGVO)

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

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

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

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 Risiken abzuwägen. Diese Aufgabe muss dynamisch betrachtet werden. Das bedeutet, dass Maßnahmen in regelmäßigen Abständen auf Aktualität zu überprüfen und gegebenenfalls anzupassen sind. Insbesondere den Aufgabenträgern, im Beispiel einer Feuerwehr der örtliche Aufgabenträger nach § 2 Absatz 1 Nr. 1 BbgBKG, und für die Beratung deren IT-Sicherheits- und Datenschutzbeauftragten, kommt hier eine bedeutende Funktion zu. Einen Überblick über den aktuellen Stand der Technik sowie geeignete organisatorische Maßnahmen können beispielsweise die „IT-Grundschutzkompendium“ 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 das Verarbeitungsverzeichnis der örtlichen Aufgabenträger (Art. 30 DSGVO) um die Verarbeitung der Einsatzdaten ergänzt werden muss. Ferner kann die Durchführung einer Datenschutz**-**Folgenabschätzung (Art. 35 DSGVO) vor der Einführung eines entsprechenden Benachrichtigungssystems erforderlich sein. Zudem ist mit Blick auf die automatisierte Datenverarbeitung gemäß § 4 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) eine Freigabe zu erteilen und die Freigabeerklärung dem Verarbeitungsverzeichnis der örtlichen Aufgabenträger beizufügen. Ein Muster für eine Freigabeerklärung findet sich in Anlage 5 der Anwendungshinweise des Ministeriums des Innern und für Kommunales (MIK) zur DSGVO und zum BbgDSG (aufrufbar unter https://mik.brandenburg.de/mik/de/ministerium/akteneinsicht-und-datenschutz/).

Rechtsfolgen bei Verstößen und Missbrauch

Der Gesetzgeber misst dem Schutz persönlicher Daten 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 Datenschutzaufsichtsbehörde und ggfs. den betroffenen Personen gemeldet werden (Art. 33, 34 DSGVO). Die Datenschutzaufsichtsbehörde kann gegenüber dem Verantwortlichen, hier also dem örtlichen Aufgabenträger, von ihren Befugnissen nach Art. 58 DSGVO (z.B. Warnungen, Verwarnungen und Anweisungen) Gebrauch machen.

Greifen einzelne Organisationsangehörige die Alarmierungsdaten eigenmächtig ab, so sind scharfe Sanktionen gegen die einzelne Person möglich. Aus einer Verletzung der datenschutzrechtlichen Bestimmungen können sich dienst-, arbeits-, ordnungswidrigkeits- oder strafrechtliche Konsequenzen ergeben. So kann die unbefugte Verarbeitung personenbezogener Daten nach § 32 BbgDSG mit einer Geldbuße bis zu 50.000 Euro oder gemäß § 33 BbgDSG als Straftat mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe geahndet werden.

Angehörige öffentlicher Feuerwehren können Beamte oder zumindest förmlich Verpflichtete sein. Sie sind daher Amtsträger oder stehen solchen gleich. Angehörige Freiwilliger Feuerwehren stehen zum Aufgabenträger in einem öffentlichen Dienstverhältnis eigener Art. Werden Daten offengelegt (beispielsweise indem sie offen einsehbar ins Internet übertragen werden), so kann sich dieser 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 ehrenamtliche Feuerwehrangehörige aus dem Feuerwehrdienst ausscheidet (vgl. § 8 Abs. 1 Nr. 1 der Verordnung über Aufnahme, Heranziehung, Zugehörigkeit und Ausscheiden der ehrenamtlichen Feuerwehrangehörigen (Tätigkeitsverordnung Freiwillige Feuerwehr – TVFF)). Die letztgenannten 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 nach § 5 i.V.m. mit § 27 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) strafbar.

Fazit

Die Alarmierung von Einsatzkräften über alternative Alarmierungssysteme, bspw. via Internet auf das Smartphone, ist nur rechtlich zulässig, wenn dies lediglich eine Ergänzung zur Alarmierung mittels Funkmeldeempfängern darstellt. 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.