Leitlinien zur Melde- bzw. Benachrichtigungspflicht nach § 109a TKG

Kommt es bei der Erbringung öffentlich zugänglicher Telekommunikationsdienste zu Verletzungen des Schutzes personenbezogener Daten, hat der Anbieter des Telekommunikationsdienstes diese Datenschutzverletzungen nach § 109a TKG zu melden. Bezüglich dieser Meldepflicht hat die EU-Kommission am 24.06.2013 technische Durchführungsmaßnahmen in Bezug auf Umstände, Form und Verfahren erlassen. Die Verordnung (EU) Nr. 611/2013 – im Folgenden: „Durchführungsverordnung" – ist am 25.08.2013 in Kraft getreten. Anders als zuvor bei § 93 Abs. 3 TKG i. V. m. § 42a BDSG hat der Gesetzgeber die Meldepflicht nicht auf bestimmte Situationen begrenzt, so dass auch vermeintlich kleinere Datenschutzverletzungen mit weniger schweren Auswirkungen den Aufsichtsbehörden mitgeteilt werden müssen. Dies betont auch die EU-Kommission in ihrer Durchführungsverordnung, nach der **alle Datenschutzverletzungen** an die zuständigen Behörden zu melden sind.

Unter Berücksichtigung dieser EU-Verordnung sollen diese Leitlinien als Handreichung für die Unternehmen die Meldung einer Datenschutzverletzung vereinfachen.

1. Meldebogen

Der vorliegende Meldebogen soll sowohl die Meldung von Datenschutzverletzungen i. S. d. § 109a TKG für die meldende Stelle als auch deren Bearbeitung durch die Aufsichtsbehörden erleichtern und beschleunigen.

Der Gesetzeswortlaut des § 109a TKG sieht vor, dass die Meldung **sowohl** an die Bundesnetzagentur (BNetzA) **als auch** an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu übermitteln ist.

Der Meldebogen befindet sich im editierbaren PDF-Format auf den Internetseiten des BfDI und der BNetzA.

Dieser muss an BfDI (per E-Mail an 109aTKG@bfdi.bund.de) und BNetzA (per E-Mail an 109a@bnetza.de oder per Fax an 0228 - 14 6414) gesandt werden. Zur sicheren Übermittlung per E-Mail stehen entsprechende PGP-Schlüssel zur Verfügung.

Der Eingang der Meldung wird dem im Meldebogen benannten Ansprechpartner bestätigt. In diesem Zusammenhang wird auch die jeweilige Meldungsnummer mitgeteilt, die für die weitere Bearbeitung und Kommunikation als Referenznummer dient. Nur wenn im Einzelfall Rückfragen zu Angaben im Meldebogen notwendig werden, wird die Aufsichtsbehörde, die die jeweilige Meldung federführend bearbeitet, weitergehend tätig. Dies könnte beispielsweise bei abweichenden Einschätzungen hinsichtlich der Schwere der Datenschutzverletzung oder des Bestehens einer Benachrichtigungspflicht gegenüber den Betroffenen der Fall sein.

2. Meldefrist

Ziel des Meldebogens ist es, eine effiziente Behandlung des Vorfalls zu ermöglichen und dadurch die potenziell negativen Folgen des Vorfalls bestmöglich zu minimieren. Hierfür ist es essenziell, dass die **initiale Meldung** schnellstmöglich erfolgt. Gemäß Art. 2 Abs. 2 der Durchführungsverordnung muss ein meldepflichtiger Vorfall **innerhalb von 24 Stunden nach Feststellung der Datenschutzverletzung** gemeldet

werden. Eine Datenschutzverletzung gilt als festgestellt, sobald der Betreiber vom Auftreten einer Sicherheitsverletzung, die zu einer Verletzung des Schutzes personenbezogener Daten geführt hat, hinreichende Kenntnis erlangt hat.

3. Nachmeldungen

Da nicht auszuschließen ist, dass zu diesem frühen Zeitpunkt noch nicht alle Informationen für eine vollständige Meldung zur Verfügung stehen, können solche Details als „bisher unbekannt“ zunächst noch offen bleiben. Eine **Nachmeldung** der noch offenen Punkte muss **so schnell wie möglich, jedenfalls aber innerhalb von drei Tagen nach der ersten Meldung** erfolgen. Sofern auch diese Zeitvorgabe nicht eingehalten werden kann, sind sämtliche nach Ablauf der drei Tage vorliegenden Informationen zu übermitteln. Darüber hinaus ist darzulegen, wieso einzelne Informationen noch nicht geliefert werden können (vgl. Art. 2 Abs. 3 der Durchführungsverordnung).

Nachmeldungen beschränken sich nicht ausschließlich auf Ergänzungen von bislang fehlenden Informationen, sondern können auch dazu dienen, Änderungen bei bereits angegebenen Informationen aufgrund neuer Erkenntnisse mitzuteilen. Da immer die zeitlich letzte Meldung als aktuell betrachtet wird, sollte darauf geachtet werden, dass der Meldebogen **auch bei Nachmeldungen komplett** ausgefüllt wird und nicht nur bislang fehlende oder zu ändernde Punkte ergänzend mitgeteilt werden. **Auch die Nachmeldungen müssen sowohl an die BNetzA als auch an den BfDI gesandt werden**.

4. Schwere der Datenschutzverletzung

Die Einschätzung der Schwere der Datenschutzverletzung soll den Aufsichtsbehörden einen ersten aussagekräftigen Einblick in die Bedeutung des gemeldeten Vorfalls ermöglichen.

Die Schwere der Datenschutzverletzung muss möglichst objektiv von der meldenden Stelle bestimmt und in eine der vorgegebenen Kategorien eingeordnet werden. Da verschiedene Faktoren (z.B. Sensibilität der Daten, Umstände der Datenschutzverletzung, etc.) Einfluss auf eine solche Bewertung haben, ist es nicht zielführend, an dieser Stelle konkrete Beispiele für die einzelnen Kategorien anzuführen. Allerdings wird im Rahmen der Bewertung durch die Aufsichtsbehörden von Folgendem ausgegangen: Eine niedrige Schwere dürfte grundsätzlich nur dann vorliegen, wenn die von der Datenschutzverletzung betroffenen Daten nur sehr unwahrscheinlich und unter großem Aufwand einen Rückschluss auf die Betroffenen erlauben; eine sehr hohe Schwere dürfte regelmäßig gegeben sein, wenn es sich um äußerst sensible Daten handelt, bei denen ohne größere Schwierigkeiten der Bezug zum Betroffenen hergestellt werden kann und/oder dem Betroffenen aufgrund des Vorfalls ein finanzieller oder reputativer Schaden droht.

Bei der Beurteilung der Schwere der Datenschutzverletzung sind grundsätzlich die Art und Sensibilität der betroffenen Daten sowie die Umstände (z. B. ob die Datenschutzverletzung von einem Täter gezielt herbeigeführt wurde oder auf einem Versehen beruht, ob die Daten öffentlich zugänglich gemacht wurden, etc.) zu berücksichtigen. Die Zugriffsmöglichkeit auf die vom Vorfall betroffenen Daten (insbes. die potenzielle Sicherung der Daten im Sinne des § 109a Abs. 1 Satz 3 TKG) hat **keinen Einfluss auf die Pflicht zur Meldung des Verstoßes an die Aufsichtsbehörden**,

sondern wirkt sich erst bei der Entscheidung über eine Benachrichtigung der Betroffenen aus.

5. Benachrichtigung an die Betroffenen

Gemäß § 109a Abs. 1 Satz 2 TKG sind die Betroffenen zu benachrichtigen, wenn anzunehmen ist, dass sie durch die Verletzung des Schutzes ihrer personenbezogenen Daten in ihren Rechten oder schutzwürdigen Interessen schwerwiegend beeinträchtigt werden.

Bei der Beurteilung, ob eine schwerwiegende Beeinträchtigung vorliegt oder zu erwarten ist, sind die Art der betroffenen Daten, die wahrscheinlichen Folgen für die Betroffenen und die Umstände der Datenschutzverletzung zu berücksichtigen (vgl. auch Art. 3 Abs. 2 der Durchführungsverordnung).

Sofern eine Benachrichtigung der Betroffenen erforderlich ist, hat sie **schnellstmöglich** und ohne unangemessene Verzögerung zu erfolgen.

Hinsichtlich des Inhaltes der Benachrichtigung an die Betroffenen gilt § 109a Abs. 2 Satz 1 TKG i. V. m. Art. 3 Abs. 4 der Durchführungsverordnung.

Können nicht alle Betroffenen identifiziert werden, können und sollten individuelle Benachrichtigungen durch eine öffentliche Anzeige in entsprechend verbreiteten Medien ergänzt werden (vgl. Art. 3 Abs. 7 der Durchführungsverordnung). In diesem Fall müssen die Anbieter öffentlich zugänglicher Telekommunikationsdienste weiterhin alle zumutbaren Anstrengungen unternehmen, um weitere Betroffene zu ermitteln und sie so bald wie möglich mit den nötigen Angaben persönlich zu benachrichtigen.

Die Benachrichtigung kann unterbleiben, wenn die betroffenen Daten durch ein als sicher anerkanntes Verschlüsselungsverfahren oder durch andere geeignete technische Vorkehrungen i. S. d. § 109a Abs. 1 TKG geschützt sind und dies gegenüber den Aufsichtsbehörden entsprechend nachgewiesen werden kann. Sofern diese Maßnahmen bereits im Rahmen des Sicherheitskonzepts dargestellt sind, kann auf die entsprechenden Passagen verwiesen werden. Eine grundsätzliche Pflicht zur Vorlage des Sicherheitskonzeptes ergibt sich aus § 109a TKG nicht.

Sollte noch nicht bekannt sein, ob die fraglichen Daten durch geeignete Vorkehrungen ausreichend geschützt sind (z. B. weil das Datenleck noch nicht lokalisiert wurde), ist eine Benachrichtigung der möglicherweise in ihren Rechten und schutzwürdigen Interessen schwerwiegend Betroffenen grundsätzlich vorzunehmen.

Eine schwerwiegende Beeinträchtigung der Rechte und schutzwürdigen Interessen der Betroffenen kann gegebenenfalls auch angenommen werden, wenn aufgrund eines Verlustes der Daten, diese bei der datenverarbeitenden Stelle nicht mehr verfügbar sind. In diesen Fällen ist eine Benachrichtigung auch dann erforderlich, wenn die Daten durch ein als sicher anerkanntes Verschlüsselungsverfahren oder durch andere geeignete technische Vorkehrungen i. S. d. § 109a Abs. 1 TKG geschützt sind.

Anders als die Benachrichtigung der Betroffenen **hat die Meldung eines Vorfalls gegenüber BNetzA und BfDI stets zu erfolgen**, unabhängig davon ob und wie die betroffenen Daten gegen einen unberechtigten Zugriff gesichert sind. Das Unterlassen einer Meldung an die Aufsichtsbehörden kann eine Ordnungswidrigkeit i. S. d. § 149 Abs. 1 Nr. 21b TKG darstellen.

6. Mitwirkung Dritter

Sofern ein TK-Anbieter im Rahmen der Diensteerbringung Daten seiner Kunden von Dritten verarbeiten lässt, die selbst in keinen direkten vertraglichen Beziehungen mit den Kunden stehen, müssen diese verpflichtet werden, im Fall einer Datenschutzverletzung unverzüglich den TK-Anbieter zu informieren, damit dieser den oben genannten Meldepflichten nachkommen kann. Diese Anforderungen gelten unabhängig davon, ob die Dritten im Wege der Auftragsverarbeitung oder aufgrund einer Funktionsübertragung für den TK-Anbieter tätig werden.

7. Verzeichnis über Vorfälle

Sämtliche Vorfälle der letzten fünf Jahre sind unter den Voraussetzungen des § 109a Abs. 3 TKG in einem Verzeichnis zu protokollieren, welches den Aufsichtsbehörden auf Nachfrage zur Verfügung zu stellen ist.