von **Dr. Sebastian Kraska**

Datenschutz-Informationspflichten bei Datenpannen nach § 42a BDSG ("Data Breach Notifications")

Stellen Unternehmen fest, dass als besonders schutzwürdig definierte Daten (z.B. Gesundheitsdaten, Konto- und Kreditkarteninformationen) unrechtmäßig an Dritte gelangt sein können (z.B. durch einen Hackerangriff oder beispielsweise den Diebstahl eines unverschlüsselten Laptops), müssen diese die Datenschutz-Aufsichtsbehörde und die Betroffenen informieren. Der folgende Beitrag gibt einen Überblick über die rechtlichen Rahmenbedingungen dieser Datenschutz-Informationspflichten.

Beitrag von Herrn Rechtsanwalt Dr. Sebastian Kraska, externer Datenschutzbeauftragter und Herrn Diplom-Jurist Michael Stolze, LL.M. LL.M.

Hintergrund

Die Meldepflicht nach § 42a BDSG wurde 2009 im Rahmen der Novellierung des Bundesdatenschutzgesetzes (BDSG) eingeführt. Sie knüpft an einen entsprechenden **Vorschlag der Europäischen Kommission** aus dem Jahr 2007 an, um eine Ausweitung des Schutzes der Privatsphäre und der personenbezogenen Daten der Bürger in der elektronischen Kommunikation zu erreichen. Die Kommission schlug hierzu u.a. die Einführung einer Meldepflicht für Datensicherheitsverstöße vor, wie es mit den "Security Breach Notification Laws" in den USA schon länger Praxis ist.

Adressat der Informationspflicht

§ 42a BDSG richtet sich an Unternehmen (§ 2 Abs. 4 BDSG) und ihnen datenschutzrechtlich gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen (§ 27 Abs. 1 Satz 1 Nr. 2 BDSG).

Rahmen der Informationspflicht

Die Informationspflicht greift zunächst nur bei dem Verlust als besonders schutzwürdig definierter Daten. Dies sind
(a) die sog. sensiblen Daten nach § 3 Abs. 9 BDSG ("Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben"),
(b) personenbezogene Daten, welche einem Berufsgeheimnis unterliegen oder sich
(c) auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen sowie
(d) personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Es spielt dabei keine Rolle, auf welche Weise Dritte Kenntnis erlangten, solange dies unrechtmäßig geschah, was der Fall ist, wenn die Betroffenen nicht zugestimmt haben und die Offenbarung weder durch Gesetz noch durch eine sonstige Rechtsvorschrift erlaubt ist.

Neben der unrechtmäßigen Kenntniserlangung durch Dritte müssen auch noch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Dies hängt von den Umständen des jeweiligen Einzelfalls ab. Wichtige Kriterien hierfür sind die Art der betroffenen Daten und die potenziellen Auswirkungen der Kenntniserlangung durch Dritte auf die Betroffenen (z. B. materielle Schäden bei Kreditkarteninformationen oder soziale Nachteile einschließlich des Identitätsbetrugs).

Auslöse-Schwelle der Informationspflicht

Das Unternehmen muss anhand von tatsächlichen Anhaltspunkten die Entscheidung treffen, ob ein meldepflichtiger Datenverlust eingetreten sein könnte. Eine sichere Feststellung ist nicht erforderlich. Ausreichend ist, wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, dass die Daten unrechtmäßig in die Hände Dritter gelangt sein könnten.
Die tatsächlichen Anhaltspunkte können z. B. aus dem eigenen Sicherheitsmanagement stammen oder auch von Hinweisen durch Strafverfolgungsbehörden oder Datenschutzbeauftragten herrühren.

Unverzügliche Offenlegung

Die Offenlegungspflicht gilt gegenüber der zuständigen Datenschutz-Aufsichtsbehörde und den Betroffenen.
Information der Aufsichtsbehörden: Stellt eine von § 42a BDSG verpflichtete Stelle einen relevanten Datenverlust fest, dann hat sie dies der zuständigen Datenschutz-Aufsichtsbehörde unverzüglich (dies bedeutet "ohne schuldhaftes Zögern", vgl. § 121 BGB) nach Bekanntwerden des Vorfalls mitzuteilen.
Die Information der Betroffenen hat unverzüglich zu erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind und/oder die Strafverfolgung nicht mehr gefährdet wird.

Empfehlungen zur Schadensminimierung

§ 42a Satz 4 BDSG verlangt im Rahmen der Benachrichtigung neben einer Darlegung der Art der unrechtmäßigen Kenntniserlangung auch Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen. Auch dies entspricht der genannten **Empfehlung der Europäischen Kommission** , welche über eine solche Empfehlung wirtschaftliche Schäden und soziale Nachteile so gering wie möglich halten möchte.

Unverhältnismäßiger Aufwand der Einzelbenachrichtigungen

Soweit die Information der Betroffenen einen unverhältnismäßigen Aufwand erfordert (insbesondere durch die Vielzahl der Fälle), tritt an ihre Stelle die Information der Öffentlichkeit. § 42a Satz 5 BDSG legt zwar keinen konkreten Informationskanal fest, doch verdeutlicht der Gesetzgeber welche Art Informationsweg er sich grundsätzlich vorstellt. So soll die Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen informiert werden oder durch eine andere, in ihrer Wirksamkeit gleich geeigneten Maßnahme.

Spannungsverhältnis von Benachrichtigungspflicht und Selbstbezichtigungsverbot

Verstößt ein Benachrichtigungsverpflichteter gegen seine Pflicht aus § 42a BDSG, dann begeht er eine Ordnungswidrigkeit (§ 43 Abs. 2 Nr. 6 BDSG) und unter Umständen auch eine Straftat (§ 44 Abs. 1 BDSG). Der strafprozessuale Grundsatz, dass niemand sich selbst zu bezichtigen hat (nemo tenetur prodere se ipsum), führt hier zu einer Kollision für den Informationspflichtigen. Gemäß § 42a Satz 6 BDSG sieht der Gesetzgeber vor, dass die Benachrichtigung bzw. die darin enthaltenen Informationen in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten nicht ohne den Willen des Benachrichtigungspflichtigen verwendet werden dürfen. Gemäß § 43 Abs. 2 Nr. 7, Abs. 3 BDSG droht ein Bußgeld von bis zu 300.000 Euro für den Fall, dass eine Benachrichtigung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgt.

Ausweitung von Informationspflichten

Der Gesetzgeber verankert die Informationspflicht nach § 42a BDSG auch mittelbar in anderen Gesetzen. Damit wird sukzessive der Rahmen der meldepflichtigen Vorfälle erweitert.

§ 93 Abs. 3 Telekommunikationsgesetz (TKG) verweist auf § 42a BDSG für den Fall, dass Bestands- und Verkehrsdaten (vgl. § 3 Nr. 3 und Nr. 30 TKG) unrechtmäßig zur Kenntnis Dritter gelangen. Adressat der Informationspflicht ist jeder Diensteanbieter (§ 3 Nr. 6 TKG).

Entsprechendes gilt nach § 15a Telemediengesetz (TMG) für Bestands- und Nutzungsdaten nach §§ 14 und 15 TMG und im Sozialrecht gemäß § 83a Sozialgesetzbuch (SGB) X für Sozialdaten nach § 67 Abs. 12 SGB X.

Fazit

§ 42a BDSG (und auf diese Vorschrift verweisende Normen) legt Unternehmen im Fall des begründeten Verdachts über den Verlust von als besonders schutzwürdig definierten Daten die Pflicht auf, die Datenschutz-Aufsichtsbehörde und die Betroffenen zu informieren. Unternehmen sollten dieser Informationspflicht mit technischen und organisatorischen Maßnahmen entgegenwirken (z.B. Einsatz von Verschlüsselungstechnik). Ferner sollten Unternehmen Prozesse etablieren, um etwaige Informationsverpflichtungen zur Meidung ordnungs- und strafrechtlicher Sanktionen zu erkennen.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt