Informationspflicht bei Datenverlust beim Postversand

Zusammenfassung: Der Verlust sensibler personenbezogener Daten, die per Post verschickt wurden, und den Empfänger nach fünf Tagen nicht erreicht haben, kann eine Informationspflicht von Aufsichtsbehörden und Betroffenen nach § 42a BDSG oder den einschlägigen Gesetzen auslösen.

Gehören Sie auch zu den meisten Unternehmen, die ihre Informationspflichten kennen, wenn Dritte unrechtmäßig von besonders sensiblen personenbezogenen Daten Kenntnis genommen haben? Der Baden-Württembergische Landesdatenschutzbeauftragte hat diese Aussage getroffen und hat hierzu offenbar eine besonders positive Meinung. Könnten Sie auf Anhieb sagen, in welchen Fällen Ihr Unternehmen dieser Informationspflicht unterliegt und was Sie dabei alles beachten müssen? Wenn das so ist, brauchen Sie nicht weiterlesen. Falls Sie ehrlich sind und nein antworten müssten, haben wir vielleicht die eine oder andere interessante Information für Sie.

Der Praxisfall: Ein Unternehmen erbringt für Dritte Dienstleistungen im Rückbau belasteter Gebäude. Die Beschäftigten unterliegen der permanenten arbeitsmedizinischen Betreuung. Ein Auftraggeber benötigt die entsprechenden arbeitsmedizinischen Bestätigungen, damit dort die Umsetzung der Dokumentations- und Prüfpflichten nachgewiesen werden kann. Die Unterlagen werden in einem Umschlag und per Nachnahme an den Auftraggeber gesendet. Die Postsendung erreicht den Auftraggeber auch nach mehreren Tagen nicht. Der Datenschutzbeauftragte des Unternehmens ist alarmiert und überlegt, ob er die zuständige Aufsichtsbehörde für den Datenschutz gemäß § 42a BDSG zu informieren hat.

Rechtslage: Stellt ein Unternehmen fest, dass Gesundheitsdaten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat es dies unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. § 42a BDSG.

Gilt das auch für Postsendungen? Diese interessante Frage hat der Landesdatenschutzbeauftragte für Baden-Württemberg in seinem 32. Tätigkeitsbericht aufgegriffen. Es heißt dort auf S. 180 des Berichts: „Eine solche Informationspflicht ist grundsätzlich zu bejahen. Zwar stellt der Wortlaut der Vorschrift darauf ab, dass die verantwortliche Stelle eine unrechtmäßige Kenntniserlangung der Daten positiv feststellt. Wollte man aber bei ungewissem Schicksal der versendeten Daten eine Informationspflicht ablehnen, so liefe dies dem Schutzzweck des § 42a BDSG zuwider. Die Meldepflicht soll beim Verlust sensibler personenbezogener Daten, deren unberechtigte Kenntnisnahme leicht zu einer schwerwiegenden Beeinträchtigung des Betroffenen führen kann, den Betroffenen und die Datenschutzaufsichtsbehörde in die Lage versetzen, negative Konsequenzen eines solchen Vorfalls abzuwenden. Dies ist nur möglich, wenn die verantwortliche Stelle mit der Meldung nicht zuwartet, bis ein endgültiger Datenverlust oder eine unberechtigte Kenntnisnahme Dritter sicher feststeht, sondern bereits die längere Nicht Auffindbarkeit der Daten meldet.“

Wann muss die Meldung erfolgen? In unserem Praxisfall sind Unterlagen über Gesundheitsuntersuchungen nach mehreren Tagen noch nicht beim Empfänger eingegangen. Es ist nicht so selten, dass Postsendungen mehrere Tage unterwegs sind. Zur Erleichterung der Betroffenen kommen die Sendungen dann eines Tages doch noch an. Wenn also auch bei nicht zugestellten Postsendungen eine Informationspflicht besteht, bleibt immer noch die Frage, wann diese eintritt. Nach wie viel Tagen Nichtzustellung ist die Informationspflicht zu erfüllen? Auch hierzu hat sich die Aufsichtsbehörde Baden-Württemberg geäußert: „Für verschollene Postsendungen gilt daher Folgendes: Erfährt die verantwortliche Stelle, dass eine Sendung mit Daten im Sinne des § 42a BDSG nach fünf Tagen, gerechnet ab dem Tag, der dem Tag der Absendung folgt, nicht beim Empfänger eingegangen ist, so hat sie die Aufsichtsbehörde und die Betroffenen nach § 42a BDSG zu informieren, wenn die Sendung nicht umgehend ausfindig gemacht werden kann. Dies gilt nicht, wenn das Ende der Frist auf einen Sonntag fällt.“

Konsequenzen für den Unternehmensalltag: zunächst könnte man meinen, die Informationspflicht kann schon nicht so schlimm sein, denn wie soll die Aufsichtsbehörde mitbekommen, wenn ein eigentlich der Informationspflicht unterliegender Fall „unter den Teppich“ gekehrt wird. Das kann sich jedoch rasch als Trugschluss herausstellen. Der Informationspflicht nicht nachzukommen, bedeutet in der Regel eine Ordnungswidrigkeit zu begehen. Ordnungswidrig handelt nach § 43 Abs. 2 BDSG, wer vorsätzlich oder fahrlässig (Ziffer 7) „entgegen § 42a Satz 1 BDSG eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht“. Das kann teuer werden: „Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit

einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden“. (§ 43 Abs. 3 BDSG).

Den Eintritt der Informationspflicht erkennen: Die eigentliche Herausforderung für Datenschutzbeauftragte und Unternehmen ist es jedoch, den Eintritt der Informationspflicht überhaupt zu erkennen. Da Postsendungen dem Briefgeheimnis unterliegen, ist das aus Sicht des Datenschutzes auch grundsätzlich kein Problem, solange die Sendungen beim Empfänger ankommen. Die Herausforderung ist nun, den Fall zu erkennen, der die Informationspflicht auslöst.

Dokumentation der kritischen Sendungen: In der Regel lässt sich diese Frage jedoch ganz pragmatisch lösen. Es ist guter Brauch in den Unternehmen, dass Sendungen mit sensiblen Informationen zumindest per Einschreiben, nicht selten auch mit Rückschein oder gar mit persönlicher Empfangsbestätigung (Postidentverfahren) versendet werden. An dieses Verfahren können sich Datenschutzbeauftragte andocken. Sie müssen erreichen, dass auch Sendungen mit personenbezogenen Daten, die eine Informationspflicht nach § 42a BDSG auslösen könnten, in dieses Verfahren einbezogen werden. Wenn die Bestätigung eingeht, dass die Sendung beim Empfänger angekommen ist, ist alles gut. Ist der Empfang der Sendung jedoch nach fünf Tagen noch nicht bestätigt, ist der Datenschutzbeauftragte zu informieren, um gegebenenfalls weitere Schritte einzuleiten.

Feststellen: Stellt eine zuständige Stelle z. B. aus dem eigenen Sicherheitsmanagement, im Wege der Benachrichtigung durch den Auftragsdatenverarbeiter, durch Hinweise Betroffener oder durch Hinweise von Strafverfolgungsorganen, fest, dass personenbezogene Daten, die zu den in § 42a genannten Datenkategorien gehören, unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten zur Kenntnis gelangt sind oder sein könnten, liegt mir großer Wahrscheinlichkeit ein Vorgang vor, der die Informationspflicht nach § 42a auslöst. Demzufolge ist intern zu definieren, wie diese Feststellung im konkreten Fall erfolgen kann.

Verfahrensvorgaben formulieren: In Ergänzung zu einer möglicherweise vorliegenden Richtlinie, in der geregelt ist, wie mit der Informationspflicht nach § 42a umzugehen ist, sollte eine Verfahrensvorgabe erstellt werden, in der das Vorgehen bei Verlust von Postsendungen mit entsprechenden Inhalten beschrieben wird. Darin sollte enthalten sein, wie die Geschäftsführung und der Datenschutzbeauftragte erfahren, dass eine Postsendung mit den Inhalten, die eine Informationspflicht auslösen, ihr Ziel nicht erreicht hat. Hier sollte die Frist von fünf Tagen zugrunde gelegt werden, die oben bei „Wann muss die Meldung erfolgen?“ beschrieben ist.

Prüfung und Meldung einleiten: In der Folge müssen Unternehmensleitung und Datenschutzbeauftragter die Prüfung einleiten, ob die Informationspflicht eingetreten ist oder nicht. Die von der Aufsichtsbehörde in Baden-Württemberg gesetzte Frist ist sehr knapp bemessen, spricht doch das Gesetz selbst von „unverzüglich“ also „ohne schuldhaftes Verzögern“. Doch auch hier kommt es auf die Umstände an. Bei einer Sendung innerhalb Deutschlands sind die fünf Tage vertretbar. Bei einer Sendung an die Tochterfirma in Italien beispielsweise wären fünf Tage zu kurz, weiß man doch aus Erfahrung, dass schon eine Urlaubspostkarte mehrere Wochen bis zur Zustellung brauchen kann. Hier sollte „unverzüglich“ näher definiert werden. Im Zweifel sollte sich der Datenschutzbeauftragte gemäß § 4g Abs. 1 BDSG an die zuständige Aufsichtsbehörde wenden.

Folgenabschätzung vornehmen: Dann ist zu prüfen, ob in der Folge des (möglichen / faktischen) Datenverlusts auch die zweite Bedingung des § 42a zutrifft. Es müssen schwerwiegende Beeinträchtigungen für die Betroffenen drohen (hohes Gefahrenpotential). Diese Folgenabschätzung ist im Idealfall schon in der Verfahrensbeschreibung vorgenommen worden, so dass hier nur auf dieser zugegriffen werden muss. Drohen tatsächlich schwerwiegende Beeinträchtigungen für die Betroffenen, muss nun auch die Information der Betroffenen in der im § 42a BDSG geforderten Weise erfolgen.

Vermeiden von Vorgängen, die eine Informationspflicht auslösen könnten: Damit der Fall der Informationspflicht gar nicht erst eintreten kann, ist auch zu prüfen, ob es zum Postversand auch Alternativen gibt. Beispielsweise kann ein persönlicher Kurier- oder Fahrdienst, wie ihn beispielsweise ärztliche Labore zum Transport von Proben und Befunden zwischen Arztpraxis und Labor einsetzen, eine sinnvolle Alternative sein.

Mitarbeiterschulungen zur Ergänzung: Wenn alle am Verfahren Beteiligten in angemessener Weise mit den Risiken und den Möglichkeiten zur Verringerung der Risiken vertraut sind, wird eine weitere Chance genutzt, Vorgänge zu vermeiden, die eine Informationspflicht von Aufsichtsbehörde und Betroffenen auslösen können.

Handlungsempfehlungen:

1. Prüfen Sie, ob im Unternehmen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, die unter die Daten fallen, deren Verlust eine Informationspflicht nach § 42a auslösen
2. Sind die Verfahrensbeschreibungen vollständig und aktuell erstellt worden, finden sich dort die entsprechenden Hinweise. Vorausschauende Datenschutzbeauftragte legen die Verfahrensbeschreibungen so an, dass § 42a-Daten auf den ersten Blick erkennbar sind.
3. Definieren Sie in einer Richtlinie zu § 42a, welche Fälle die Informationspflicht auslösen können.
4. Falls erforderlich, legen Sie für jeden der Fälle fest, wann welche Meldung an den Datenschutzbeauftragten bzw. die Unternehmensleitung erfolgen muss.
5. Prüfen Sie, ob der Verlust von Postsendungen mit 42a-Daten in der Richtlinie vorkommt. Wenn nicht, nehmen Sie diesen Fall mit auf.
6. Prüfen Sie zusammen mit den Verfahrensverantwortlichen, ob die Übermittlungswege dem Risiko angemessen gewählt wurden.
7. Legen Sie zusammen mit den Verantwortlichen eine Frist fest, nach der je nach Umständen die Sendung als unsicher hinsichtlich der Zustellung gelten muss.
8. Definieren Sie interne Meldewege.
9. Legen Sie Prüfkriterien fest, mit denen ohne weiteren Zeitverlust festgestellt werden kann, ob die Informationspflicht eingetreten ist oder nicht.
10. Stimmen Sie sich mit der Geschäftsführung ab und nehmen Sie die Informationsplicht de Aufsichtsbehörde und der Betroffenen vor.
11. Prüfen Sie, ob Sie durch Prozessänderung eine n künftigen Datenverlust möglicherweise verhindern können. Wenn das so ist, sollten Sie entsprechende Maßnahmen ergreifen.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de