693/14/DE
WP 213

Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten

Angenommen am 25. März 2014

Zusammenfassung

Mit dieser Stellungnahme möchte die Artikel-29-Datenschutzgruppe den für die Verarbeitung Verantwortlichen Leitlinien an die Hand geben, mit denen sie leichter entscheiden können, ob im Falle einer „Verletzung des Schutzes persönlicher Daten“ die betroffenen Personen benachrichtigt werden müssen. Obwohl sich diese Stellungnahme mit der für die Betreiber elektronischer Kommunikationsnetze geltenden Verpflichtung gemäß Richtlinie 2002/58/EG befasst, werden vor dem Hintergrund des Entwurfs der Datenschutzverordnung Beispiele aus verschiedenen Bereichen betrachtet und bewährte Verfahren vorgestellt, die von allen für die Verarbeitung von Daten Verantwortlichen angewendet werden können.

Während die Benachrichtigung der zuständigen Behörde gemäß Richtlinie 2002/58/EG für alle Datenschutzverletzungen vorgeschrieben ist, werden in dieser Stellungnahme Verletzungen des Schutzes personenbezogener Daten analysiert, die den betroffenen Personen gemeldet werden müssen. Dabei wird erörtert, wie die für die Verarbeitung Verantwortlichen bei der Einrichtung ihres Systems hätten vorgehen können, um Verletzungen des Schutzes personenbezogener Daten von vornherein zu vermeiden, bzw. welche Maßnahmen sie im Vorfeld hätten ergreifen können, um zumindest auf eine Benachrichtigung der betroffenen Personen verzichten zu können.

In der Stellungnahme werden außerdem einige der wichtigsten Fragen beantwortet, die im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten und der Anwendung der Richtlinie 2002/58/EG bestehen.

1. Einleitung

Der Begriff „Verletzung des Schutzes personenbezogener Daten“ wird in Artikel 2 Buchstabe i) der Richtlinie 2002/58/EG definiert als „Verletzung der Sicherheit, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in der Gemeinschaft verarbeitet werden.“

Die Richtlinie 2002/58/EG (und ebenso die vorgeschlagene Datenschutzverordnung der EU) schreibt vor, dass Verletzungen des Schutzes personenbezogener Daten der zuständigen nationalen Behörde gemeldet werden. Die genauen Vorgaben zum Inhalt dieser Meldungen sind Anhang I der Verordnung (EU) Nr. 611/2013 zu entnehmen.

Wenn anzunehmen ist, dass durch die Verletzung des Schutzes personenbezogener Daten die personenbezogenen Daten einer Person oder deren Privatsphäre beeinträchtigt werden, so benachrichtigt der Betreiber auch die betroffene Person[1] ohne unangemessene Verzögerung[2] von der Verletzung.

Sowohl die Richtlinie 2002/58/EG als auch die Verordnung (EU) Nr. 611/2013 sehen eine Ausnahme von der Pflicht zur Benachrichtigung der betroffenen Personen vor, wenn die Daten unverständlich gemacht wurden. Hat der Betreiber zur Zufriedenheit der zuständigen nationalen Behörde nachgewiesen, dass er geeignete technische Schutzmaßnahmen getroffen hat, um die Daten für alle Personen, die keine Zugriffsberechtigung haben[3], unverständlich zu machen, und wurden diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet, so braucht er die betroffenen Personen nicht über die Verletzung des Schutzes personenbezogener Daten zu benachrichtigen[4].

Der Grund für diese Befreiung von der Pflicht zur Benachrichtigung der betroffenen Personen besteht darin, dass die Restrisiken für die Privatsphäre der Betroffenen durch angemessene Maßnahmen auf ein vernachlässigbares Maß verringert werden können. Dessen ungeachtet stellt eine Verletzung der Vertraulichkeit personenbezogener Daten, die durch einen dem Stand der Technik entsprechenden Algorithmus verschlüsselt wurden, eine Verletzung des Schutzes personenbezogener Daten dar und muss daher der zuständigen Behörde gemeldet werden. Sofern die Vertraulichkeit des Schlüssels gewahrt ist, sind die Daten jedoch grundsätzlich für unbefugte Personen unverständlich. Es ist folglich davon auszugehen, dass

[1] In dieser Stellungnahme wird der Begriff „betroffene Person“ im Sinne der Richtlinie 95/46/EG verwendet. Im Zusammenhang mit der Richtlinie 2002/58/EG entspricht dies dem Begriff „Teilnehmer oder Person“.

[2] Gemäß Richtlinie 2002/58/EG und Verordnung (EU) Nr. 611/2013 wird die zuständige Behörde binnen 24 Stunden nach Feststellung der Verletzung des Schutzes personenbezogener Daten benachrichtigt, soweit dies möglich ist. Diese Frist kann in bestimmten Fällen auf 72 Stunden verlängert werden. Die Benachrichtigung des Teilnehmers oder der Person muss ohne unangemessene Verzögerung (im Sinne des Artikels 2 Absatz 2 der Verordnung (EU) Nr. 611/2013) nach Feststellung der Verletzung des Schutzes personenbezogener Daten erfolgen. Sie erfolgt unabhängig von der Meldung bei der zuständigen nationalen Behörde.

[3] Richtlinie 2002/58/EG, Artikel 4 Absatz 3; Verordnung (EU) Nr. 611/2013, Artikel 4 Absatz 1; Datenschutz-Grundverordnung, nichtamtliche konsolidierte Fassung, bereitgestellt vom Berichterstatter nach der Abstimmung im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE), Artikel 32 Absatz 3.

[4] Dabei ist Folgendes zu beachten: Sollte die Sicherheit des Schlüssels zu einem späteren Zeitpunkt beeinträchtigt werden, müssen alle zurückliegenden Verletzungen, die aufgrund der Vertraulichkeit des Schlüssels nicht gemeldet wurden, gemeldet werden.

die betroffenen Personen durch die Datenschutzverletzung nicht beeinträchtigt werden und somit nicht benachrichtigt werden müssen.

Doch selbst wenn die Daten verschlüsselt sind, kann der Verlust oder die Änderung der Daten die betroffenen Personen beeinträchtigen, wenn der für die Datenverarbeitung Verantwortliche über keine angemessene Sicherungskopie der Daten verfügt. In diesem Fall sollten die betroffenen Personen benachrichtigt werden, selbst wenn die Daten durch Verschlüsselungsmaßnahmen geschützt wurden.

Es ist deshalb wichtig, dass die für die Verarbeitung Verantwortlichen vorausschauend planen und handeln. Gemäß Artikel 17 der Richtlinie 95/46/EG sowie gemäß Artikel 4 Absätze 1 und 1a der Richtlinie 2002/58/EG müssen die für die Verarbeitung Verantwortlichen geeignete technische und organisatorische Maßnahmen ergreifen, um ein Sicherheitsniveau zu gewährleisten, das den von der Datenverarbeitung ausgehenden Risiken angemessen ist. Zu diesem Zweck ist es wichtig, dass ein angemessener Rahmen für das Risikomanagement zur Verfügung steht. Dieser Rahmen muss die Mindestelemente eines solchen Ansatzes aufweisen und angemessene Mindestanforderungen an die technischen und organisatorischen Kontrollen enthalten, die der für die Verarbeitung Verantwortliche festlegen kann. Dabei ist ein besonderer Schwerpunkt auf solche Maßnahmen zu legen, die die Daten erforderlichenfalls unverständlich machen. Unternehmen sollten außerdem im Vorfeld geeignete Pläne für den Umgang mit etwaigen Verletzungen des Schutzes personenbezogener Daten festlegen, um sicherzustellen, dass rasch und wirksam auf eine solche Verletzung reagiert werden kann.

Wenn Artikel 17 angemessen berücksichtigt wurde, d. h. wenn vor Beginn der Datenverarbeitung geeignete Sicherheitsmaßnahmen getroffen wurden, ist davon auszugehen, dass die mit einer Verletzung des Schutzes personenbezogener Daten verbundenen Risiken im Voraus analysiert und gemindert wurden. In solchen Fällen dürfte es seltener zu Verletzungen des Schutzes personenbezogener Daten kommen, und etwaige Verletzungen dürften die betroffenen Personen weniger beeinträchtigen. Da eine Benachrichtigung der betroffenen Personen nicht erforderlich ist, wenn die Verletzung die personenbezogenen Daten oder die Privatsphäre der betroffenen Personen nicht beeinträchtigt, oder wenn geeignete technische Schutzmaßnahmen in Bezug auf die von der Verletzung betroffenen Daten getroffen wurden, kann eine Benachrichtigung am besten dadurch vermieden werden, dass in den Projekten, in denen personenbezogene Daten verarbeitet werden, angemessene Vorkehrungen für den Schutz der Privatsphäre getroffen werden.

Die Benachrichtigung der betroffenen Personen sollte ohne unangemessene Verzögerung[5] und unabhängig von der Meldung der Verletzung des Schutzes personenbezogener Daten bei der zuständigen nationalen Behörde erfolgen. Dabei sollte der für die Datenverarbeitung Verantwortliche berücksichtigen, dass der wichtigste Nutzen einer Benachrichtigung darin besteht, dass die betroffenen Personen die notwendigen Informationen erhalten, um negative Auswirkungen, die sich aus den Umständen der Datenschutzverletzung ergeben können, zu verringern, auch wenn dies kein Entscheidungskriterium für oder gegen die Benachrichtigung darstellt. Bestehen von Seiten des für die Verarbeitung Verantwortlichen Zweifel hinsichtlich der Wahrscheinlichkeit einer Beeinträchtigung der personenbezogenen Daten oder der

[5] Gemäß Richtlinie 2002/58/EG und Verordnung (EU) Nr. 611/2013 wird die zuständige Behörde binnen 24 Stunden nach Feststellung der Verletzung benachrichtigt, soweit dies möglich ist. In bestimmten Fällen kann diese Frist auf 72 Stunden verlängert werden. Die Benachrichtigung des Teilnehmers oder der Person muss ohne unangemessene Verzögerung nach Feststellung der Verletzung des Schutzes personenbezogener Daten erfolgen.

Privatsphäre der betroffenen Personen, so sollte er die Personen sicherheitshalber benachrichtigen. Darüber hinaus sollte er die Möglichkeit bedenken, dass die zuständigen Behörden nach genauerer Prüfung der Meldung die Benachrichtigung der Personen verlangen können.

In der vorliegenden Stellungnahme wird eine **nicht erschöpfende Liste von Beispielfällen vorgestellt, in denen die betroffenen Personen benachrichtigt werden sollten.**[6] Jede Verletzung des Schutzes personenbezogener Daten wird dabei im Hinblick auf die drei klassischen Sicherheitskriterien „Verfügbarkeit", „Integrität " und „Vertraulichkeit" der Daten analysiert. Unter einer „Verletzung der Verfügbarkeit" versteht man somit den Verlust oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten, unter einer „Verletzung der Integrität" versteht man die Änderung personenbezogener Daten und unter einer „Verletzung der Vertraulichkeit" die unbefugte Preisgabe oder Einsichtnahme in personenbezogene Daten. Daran schließen sich **allgemeine Hinweise** zu Fällen an, in denen eine Meldung unterbleiben kann. Abschließend werden die **wichtigsten Aspekte erörtert**, mit denen die für die Verarbeitung Verantwortlichen konfrontiert sein können, wenn sie prüfen, ob eine Benachrichtigung der betroffenen Personen erforderlich ist.

[6] Da die vorgeschlagene Datenschutzverordnung vorsieht, die Meldepflicht auf alle Sektoren auszudehnen, und in mehreren Ländern bereits eine gesetzliche Meldepflicht besteht, beschränken sich die in dieser Stellungnahme erörterten Beispiele nicht auf den Bereich der elektronischen Kommunikation.

2. Datenschutzverletzungen, die die betroffenen Personen beeinträchtigen können

Verletzungen sollten den betroffenen Personen unverzüglich gemeldet werden, wenn anzunehmen ist, dass ihre personenbezogenen Daten oder ihre Privatsphäre beeinträchtigt werden. In diesem Abschnitt werden Beispiele für Verletzungen aufgeführt, bei denen dieses Kriterium zutrifft. Es werden außerdem Beispiele für technische Maßnahmen vorgestellt, die im Fall ihrer Anwendung vor dem Verstoß eine Benachrichtigung der betroffenen Personen unter Umständen hätten verzichtbar machen können.

Fall 1: *Aus einer Gesundheitseinrichtung für Kinder wurden vier Laptop-Computer gestohlen; sie enthielten sensible Gesundheits- und Sozialdaten sowie andere personenbezogene Daten von 2050 Kindern.*

Diese Verletzung des Schutzes personenbezogener Daten betrifft die Vertraulichkeit und (sofern der für die Verarbeitung Verantwortliche auf keine Sicherungskopie der Daten zurückgreifen kann) die Verfügbarkeit und Integrität der Daten.

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Es handelt sich primär um eine Verletzung der ärztlichen Geheimhaltungspflicht. Die Datenbank enthält vertrauliche medizinische Informationen über die Kinder, die von Unbefugten eingesehen werden können.
- Die Veröffentlichung dieser Daten kann sich auf das schulische und/oder familiäre Umfeld der Kinder auswirken (z. B. Informationen über gewalttätige Übergriffe, chronische Krankheiten, psychische Probleme, soziale oder finanzielle Schwierigkeiten der Familie usw.).
- Kinder und Eltern können emotional beeinträchtigt werden.
- Die Daten können dazu verwendet werden, Eltern und Kinder (je nach ihrem Alter) zu erpressen.
- Die Eltern schwer kranker Kinder könnten gezielt von Personen kontaktiert werden, die versuchen, aus der Kenntnis der Lebensumstände der Betroffenen Nutzen zu ziehen (Scharlatane, Sekten usw.).

Mögliche negative Folgen, die sich aus der Verletzung der Verfügbarkeit ergeben können:

- Die Verletzung der Datenverfügbarkeit kann die Kontinuität der Behandlung der Kinder gefährden und eine Verschlimmerung der Krankheit oder einen Rückfall herbeiführen.
- Sie kann zu einer versehentlichen Vergiftung führen, wenn Medikamentenallergien vorliegen oder Medikamente verabreicht werden, die sich nicht miteinander vertragen. Dies kann verschiedene gesundheitliche Probleme bis zum Tod zur Folge haben.

- Sie kann zu unangemessenen Verzögerungen bei der Kostenerstattung oder der finanziellen Unterstützung für die betroffenen Personen führen, was sich negativ auf die finanzielle Situation der betroffenen Familien auswirken kann.

Mögliche negative Folgen, die sich aus der Verletzung der Integrität ergeben können:

- Der Verlust der Daten kann die Integrität der medizinischen Unterlagen beeinträchtigen, was sich negativ auf die Behandlung der Kinder auswirken kann. Wenn zum Beispiel nur eine ältere Sicherungskopie der Patientenakten vorhanden ist, sind alle Änderungen, die an den Daten auf den gestohlenen Computern vorgenommen wurden, verloren. Dies beeinträchtigt die Korrektheit der Daten. Die Verwendung von Patientenakten, die nicht auf dem aktuellsten Stand sind, kann die Kontinuität der Behandlung der Kinder gefährden und zu einer Verschlimmerung der Krankheit oder einem Rückfall führen.

Aufgrund der möglichen Auswirkungen sollte in diesem Fall eine Benachrichtigung erfolgen. Es ist jedoch wichtig, dass dabei das Alter und die Reife der betroffenen Personen berücksichtigt werden. Es kann in diesem Fall angemessener sein, zusätzlich zur Benachrichtigung der Kinder selbst, sofern diese nach geltendem Recht angemessen oder notwendig ist, die Eltern oder die gesetzlichen Vormunde zu informieren, die bereits aktiv in die medizinische Betreuung des Kindes eingebunden sind.

Auf diese Weise können die benachrichtigten Eltern die Kontinuität der Behandlung überprüfen und auf Abweichungen hinweisen; sie können kontrollieren, welche Allergien in der Einrichtung bekannt sind oder neue medizinische Untersuchungen verlangen, um sicherzustellen, dass die Kinder die richtige Behandlung erhalten. Sie können auch beschließen, weitere Personen über den Zustand der Kinder zu informieren, um die Auswirkungen auf das Umfeld der Kinder in gewissem Umfang zu steuern.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Die Verletzung der Verfügbarkeit und Integrität der Daten hätte verhindert bzw. die daraus erwachsenden Folgen hätten gemindert werden können, wenn eine hinreichend aktuelle Sicherungskopie der Datenbestände zur Verfügung gestanden hätte.
- Die etwaigen negativen Auswirkungen der Verletzung der Vertraulichkeit hätten durch die Verwendung eines geeigneten Produkts zur Datenverschlüsselung gemindert werden können. Der Schlüssel des Verschlüsselungsprodukts muss hinreichend stark und geheim sein.

Wären solche Sicherheitsvorkehrungen getroffen worden und wäre ihre Sicherheit gewährleistet (d. h. bliebe der Schlüssel geheim und stünde eine Sicherungskopie zur Verfügung), so kann die Benachrichtigung der betroffenen Personen im Prinzip unterbleiben. Dies sollte der zuständigen Behörde zu ihrer Zufriedenheit nachgewiesen werden.

Fall 2: *Durch die Ausnutzung einer Schwachstelle in einer Web-Anwendung erlangten Unbefugte Zugang zu den personenbezogenen Kundendaten eines Lebensversicherungsmaklers. Die Daten enthielten Namen und Anschrift der betroffenen Personen und die von ihnen ausgefüllten medizinischen Fragebogen. 700 Personen waren betroffen.*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Daten, die der Angreifer im Internet veröffentlicht, können die Chancen der Betroffenen, Beschäftigung zu finden, beeinträchtigen (z. B. Angaben zu Gesundheitsproblemen, Schwangerschaft usw.).
- Die betroffenen Personen können in ihrem beruflichen und/oder familiären Umfeld beeinträchtigt werden.
- Auch emotionale Auswirkungen können auftreten, wenn die betroffenen Personen ihre Diagnose geheim gehalten haben.
- Es kann zu Identitätsbetrug kommen.
- Die Daten (z. B. Informationen darüber, Kunde eines Unternehmens zu sein oder für bestimmte Dienstleistungen zu bezahlen) können für das Abgreifen von Passwörtern (Phishing) benutzt werden.

Da anzunehmen ist, dass die betroffenen Personen durch diese Datenschutzverletzung beeinträchtigt werden, müssen sie benachrichtigt werden.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Eine kontinuierliche Überwachung der verwendeten Technologien auf mögliche Schwachstellen, darunter unter anderem regelmäßiges Scannen auf Sicherheitslücken der Website und Aktualisierung der Software (einschließlich der Sicherheitssoftware), hätten die Verletzung verhindern oder deren Auswirkungen begrenzen können.

  Auch wenn sich Sicherheitsschwachstellen, die der Öffentlichkeit oder dem Produktanbieter noch unbekannt sind („Zero-Day-Exploits“), nicht leicht vermeiden lassen, kann das mit ihnen verbundene Risiko durch geeignete vorausschauende und wirksame Maßnahmen, die verhindern, dass Sicherheitslücken ausgenutzt werden, auf ein akzeptables Niveau gesenkt werden. Wirksame Strategien für die Behandlung von Sicherheitsvorfällen können außerdem dazu beitragen, die Folgen einer Datenschutzverletzung zu mindern, indem die Dauer und Tragweite der negativen Auswirkungen begrenzt werden.

- Wie im vorigen Fall hätten die möglichen negativen Folgen der Vertraulichkeitsverletzung durch die Verwendung eines geeigneten Verschlüsselungsprodukts, das die Kundendaten mit Hilfe eines hinreichend starken und geheimen Schlüssels schützt, gemindert werden können. Eine solche Maßnahme kann insbesondere bei einem Diebstahl der Festplatte oder ähnlichen Verstößen einen wirksamen Schutz darstellen.

- Schließlich hätte die Versicherungsgesellschaft verschiedene Technologien zum Schutz der Privatsphäre einsetzen können. Dabei wird die Verarbeitung personenbezogener Daten auf ein Mindestmaß beschränkt und/oder die Identifizierbarkeit der betroffenen Person erschwert. So hätte die Versicherungsgesellschaft ihren Kunden beispielsweise per Post eine zufallsgenerierte Identifikationsnummer zusenden können, die es ihnen erlaubt

hätte, den medizinischen Fragebogen online auszufüllen. Auf diese Weise können Fragen nach dem Namen, der Adresse, dem Geburtsdatum oder der Telefonnummer im Online-Fragebogen vermieden werden.

Fall 3: *Ein Angestellter eines Internetdienstanbieters hat einem Dritten den Anmeldenamen und das Passwort für ein Benutzerkonto mit umfassenden Zugangsrechten zur Kundendatenbank überlassen. Über dieses Benutzerkonto kann der Dritte unbeschränkt auf alle Kundeninformationen zugreifen. Die Datenbank enthält neben den Namen, Adressen, E-Mail-Adressen, Telefonnummern und anderen die Personen identifizierenden Daten die Zugangsdaten der Kunden (Benutzernamen, „gehashte" Passwörter, Kundennummern) sowie deren Zahlungsdaten (Bankangaben, Kreditkartennummern usw.). Obwohl die Zahlungsdaten mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt waren, hatte der Dritte über das durch die Sicherheitsverletzung beeinträchtigte Hauptbenutzerkonto Zugang zu diesem Algorithmus. Das Unternehmen hat mehr als 100 000 Kunden.*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Ein Missbrauch der Zahlungsdaten (insbesondere der Kreditkartenangaben) hätte negative finanzielle Auswirkungen auf die Kunden.
- Da die Passwörter nur „gehasht" waren, kann der entsprechende Klartext leicht daraus abgeleitet werden. Der Zugang zu den Kundenkonten wäre selbst nach Sperrung der von der Sicherheitsverletzung betroffenen Konten weiterhin möglich.
- Mit Hilfe der E-Mail-Adressen und Passwörter könnte der Dritte leicht auf andere Online-Konten betroffener Personen zugreifen, da viele Menschen für verschiedene Online-Dienste dasselbe Passwort verwenden.

Mögliche negative Folgen, die sich aus der Verletzung der Integrität ergeben können:

- Der Dritte hatte unbeschränkten Zugang zur Datenbank und kann Kontodaten geändert, gelöscht oder hinzugefügt haben.
    - Wenn das Leistungsangebot des Internetdienstanbieters auch E-Mail- und Webhosting-Dienste umfasste, könnte der Dritte diese Inhalte eingesehen, geändert oder gelöscht, DNS-Einstellungen geändert oder die Konten betroffener Personen gelöscht haben.

Obwohl die finanziellen Daten verschlüsselt waren, hatte der Dritte über die Benutzerschnittstelle Zugang zu den entschlüsselten Daten, so dass die Ausnahme von der Meldepflicht nicht gilt.

Wenn die geschützten Protokolldateien vertrauenswürdig (d. h. unbeeinträchtigt von Sicherheitsverletzungen) sind und aus den Protokolldateien ersichtlich ist, dass von dem Konto nicht auf die Kundendatenbank zugegriffen wurde, kann die Benachrichtigung der betroffenen Personen unterbleiben.

In allen anderen Fällen sollten die betroffenen Personen benachrichtigt werden, da von negativen Auswirkungen auszugehen ist und die Ausnahme von der Meldepflicht somit nicht gilt.

Immer wenn die Sicherheit von Passwörtern nicht mehr gewährleistet ist, sollten die für die Datenverarbeitung Verantwortlichen die betroffenen Personen zuverlässig dazu verpflichten, ein neues Passwort zu erzeugen. Dabei müssen sie sicherstellen, dass alle neuen Passwörter von den rechtmäßigen Benutzern und nicht von Dritten, die Zugang zu den Anmeldedaten erhielten, eingegeben werden. In der Praxis kann dies auf demselben sicheren Weg erfolgen, auf dem vergessene Passwörter erneuert werden. Bei der Aufforderung, das Passwort zu erneuern, sollte den Betroffenen der Grund mitgeteilt werden. Die Mitteilung an die Benutzer sollte die Empfehlung enthalten, nicht das vorherige Passwort oder ein ähnliches zu verwenden. Sie sollten darüber hinaus aufgefordert werden, das nicht mehr sichere Passwort in allen Konten, in denen es benutzt wurde, zu ändern.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Jedem Benutzer muss ein eigenes Konto zugewiesen werden. Der Zugang zu personenbezogenen Daten sollte ausschließlich nach dem Grundsatz „Kenntnis nur, wenn nötig“ („Need-to-know“) sowie nach dem Prinzip der geringsten Rechte („Least-Privilege“) gewährt werden. Dies gilt auch in Bezug auf Dienstleister, Wartungspersonal von Drittfirmen und andere Personen, die vorübergehend Zugang zur Datenbank benötigen. Sie sollten ausschließlich Zugang zu den Funktionen und Daten erhalten, die notwendig sind, damit sie die ihnen übertragenen Aufgaben ausführen können. Der Zugang sollte außerdem zeitlich streng befristet sein. Die Verwendung von Konten mit „globalen Zugangsrechten“ zur Datenbank sollte eingeschränkt und Verfahren zur Nachverfolgung und Beschränkung der Verwendung solcher Konten sollten eingeführt werden. Solche Sicherheitsvorkehrungen hätten die Verletzung verhindern oder deren Auswirkungen mindern können.
- Wenn die Passwörter sicher gespeichert worden wären (z. B. unter Hinzufügung eines als „Salt“ bezeichneten Zufallswertes und unter Anwendung einer kryptografischen Hash-Funktion), hätte dies die sekundären Auswirkungen für die Betroffenen erheblich verringert. Personen mit schlecht gewählten Passwörtern können trotz solcher Maßnahmen weiterhin gefährdet sein, insbesondere dann, wenn sie dieselben Zugangsdaten für verschiedene Online-Dienste verwenden. Dieses Risiko könnte dadurch verringert werden, dass die Benutzer zur Wahl eines sichereren Passworts angehalten werden.

Fall 4: *Ein Umschlag mit Kreditkartenbelegen wurde versehentlich in den Papierkorb geworfen, anstatt sicher vernichtet zu werden. Der Papierkorb wurde in einen außerhalb der Geschäftsräume zur Müllabholung aufgestellten Abfallbehälter geleert. Ein Passant nahm den Umschlag aus dem Müll und verteilte die Kreditkartenbelege in einer benachbarten Wohnsiedlung. Die Daten enthielten den Namen und die vollständigen Kreditkartenangaben[7] der Karteninhaber. In einigen Fällen enthielten die Belege sogar die Unterschrift des Karteninhabers. 800 Personen waren betroffen.*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Die Verletzung kann negative finanzielle Auswirkungen auf die betroffenen Personen haben, wenn die Daten der Zahlungskarte noch gültig sind und missbraucht werden.[8]

Da anzunehmen ist, dass die betroffenen Personen durch die Verletzung beeinträchtigt werden, müssen sie benachrichtigt werden. Wenn keine anderen Unterlagen aufbewahrt wurden, scheint es in diesem Fall schwierig, die betroffenen Personen zu benachrichtigen, da möglicherweise nicht bekannt ist, welche Kreditkartenbelege sich im Einzelnen im Umschlag befanden. Das Geschäft sollte die mit der Zahlungsabwicklung beauftragte Firma von dem Vorfall in Kenntnis setzen, damit sie den Zahlungsverkehr auf mögliche betrügerische Transaktionen überwachen kann. Ein weiteres pragmatisches Vorgehen, das sich in diesem Fall anbietet, wird in der Verordnung (EU) Nr. 611/2013 vorgeschlagen[9]: „Kann der Betreiber, [...] obwohl er hierzu alle zumutbaren Anstrengungen unternommen hat, innerhalb der in Absatz 3 genannten Frist nicht alle Personen ermitteln, die von der Verletzung des Schutzes personenbezogener Daten wahrscheinlich beeinträchtigt werden, so kann er diese Personen durch Bekanntmachungen in großen nationalen oder regionalen Medien der betreffenden Mitgliedstaaten innerhalb dieser Frist benachrichtigen." Im Falle eines Geschäfts, dessen Kunden vorwiegend aus der näheren Umgebung stammen, kann die Bekanntmachung in einer regionalen Zeitung als ausreichend erachtet werden. Ein weiterer nützlicher Schritt, um die Kunden zu schützen, könnte darin bestehen, die Kreditkartengesellschaften über die Datenschutzverletzung zu informieren.

Wenn der für die Datenverarbeitung Verantwortliche den Umschlag aus dem Papierkorb/dem Abfallbehälter herausgeholt hätte und der Umschlag nicht geöffnet worden wäre, sind negative Auswirkungen auf die Karteninhaber nicht anzunehmen. Eine Benachrichtigung der Betroffenen kann also unterbleiben.

[7] Zwar ist es bewährte Praxis, die Daten der Zahlungskarte auf den ausgedruckten Kundenbelegen zu verstümmeln, doch enthalten nicht alle Zahlungsterminals bei den Händlern diese Funktion. Es kann deshalb vorkommen, dass die Zahlungskartendaten vollständig auf den Belegkopien der Händler aufgedruckt sind.

[8] Da es immer noch Möglichkeiten gibt, Kreditkartendaten ohne Kartenprüfnummer (oder einen gleichwertigen Sicherheitscode) zu verwenden, müssen auch Datenschutzverletzungen, die nicht die Kartenprüfnummer betreffen, gemeldet werden.

[9] Dieser Vorschlag kann nützlich sein, auch wenn die Verordnung in diesem Zusammenhang keine Anwendung findet.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Das Risiko einer solchen Verletzung dürfte sowohl durch die Information der Mitarbeiter über die möglichen Folgen solcher Verstöße als auch durch den Einsatz eines geeigneten Büro-Aktenvernichters[10], bzw. eines entsprechenden Dienstleisters, zur Vernichtung der Kreditkartenbelege (und ähnlicher Belege mit personenbezogenen Daten) vor dem Wegwerfen erheblich reduziert werden.
- Die Verwendung von Zahlungsterminals, die nicht die vollständigen Kreditkartenangaben erfassen.

Fall 5: *Aus dem Kofferraum eines Fahrzeugs wurde der mit einer Verschlüsselungstechnologie geschützte Laptop eines Finanzberaters gestohlen. Auf dem Laptop befanden sich die Daten von 1000 Personen, die Angaben zu ihren finanziellen Verhältnissen (Hypotheken, Einkommen und Darlehensanträgen) gemacht hatten. Das für die Verschlüsselung verwendete Kennwort blieb geheim, doch steht keine Sicherungskopie der Daten zur Verfügung.*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Je nachdem, welche Daten genau von der Verletzung des Datenschutzes betroffen sind, kann ein Missbrauch die betroffenen Personen auf verschiedene Weise beeinträchtigen. Da die Festplatte des Laptops jedoch mit Hilfe einer dem Stand der Technik entsprechenden Verschlüsselungstechnologie unter Verwendung eines unversehrt gebliebenen starken Kennworts verschlüsselt war, kam es zu keiner unbefugten Offenlegung der Daten.

Mögliche negative Folgen, die sich aus der Verletzung der Verfügbarkeit ergeben können:

- Aufgrund des Verlusts der Daten müssen die betroffenen Personen die nötigen Angaben erneut machen. Dies hat für die Betroffenen geringfügige negative Auswirkungen in Form von Zeitverlust und Ärger zur Folge.
- In einigen Fällen kann der Verlust der Daten aber auch dazu führen, dass Fristen für die Abgabe von Anträgen oder Unterlagen versäumt werden, was je nach den Umständen verschiedene sekundäre Auswirkungen haben kann, z. B. Geldstrafen, Verlust von Einnahmen oder erwarteten Gewinnen, versäumte Chancen, Auflösung eines Kaufvertrags.

[10] Zum Beispiel ein Aktenvernichter für Papierdatenträger der Schutzklasse 2 mit der Sicherheitsstufe 4 oder höher gemäß der Norm DIN 66399.

Aufgrund des Datenverlusts und der mangelnden Vorkehrungen zur Minderung der daraus resultierenden Auswirkungen ist davon auszugehen, dass die betroffenen Personen durch diese Verletzung des Schutzes personenbezogener Daten beeinträchtigt werden. Die Verletzung ist den betroffenen Personen daher mitzuteilen. In der Benachrichtigung sollten die Betroffenen zum einen darauf hingewiesen werden, dass sie dem Finanzberater erneut Angaben machen müssen, zum anderen sollten sie über die verschiedenen negativen Folgen informiert werden, die sich aus der Verletzung ergeben können.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Eine wirksame und sichere Form der Datensicherung hätte es erlaubt, die Daten wiederherzustellen. Wenn eine aktuelle Sicherungskopie der Daten zur Verfügung gestanden hätte, wäre es zu keiner Verletzung der Datenverfügbarkeit gekommen und eine Benachrichtigung hätte unterbleiben können.

Fall 6: *Der Betreiber eines Mobilfunknetzes bietet den Teilnehmern auf seiner Website die Möglichkeit, über ein Online-Benutzerkonto die neueren Rechnungen und Kontoaktivitäten einzusehen. Ein unrechtmäßiger Zugang zu der Datenbank, in der die Passwörter für die Website gespeichert sind, wurde festgestellt. Die unbefugte Person verschaffte sich Zugang zu den Authentisierungsdaten der Benutzer (Benutzernamen und MD5-gehashte Passwörter ohne Salt).*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Die unbefugte Person kann die Passwörter ableiten und somit auf die Konten aller Kunden zugreifen, da er auch die Benutzernamen besitzt.
- Da viele Menschen dieselbe Kombination von Benutzernamen und Passwort für verschiedene Online-Konten verwenden, ist davon auszugehen, dass bei einigen Betroffenen auch der Zugang zu anderen Online-Konten, einschließlich E-Mail-Konten, gefährdet ist.

Da die Passwörter nur gehasht waren, können sie nicht als unverständlich im Sinne des Artikels 4 Absatz 2 der Verordnung (EU) Nr. 611/2013 der Kommission[11] gelten. Die Ausnahme von der Verpflichtung, die betroffenen Personen zu benachrichtigen, gilt hier also nicht.

Da anzunehmen ist, dass die betroffenen Personen durch diese Verletzung beeinträchtigt werden und die Ausnahme von der Meldepflicht somit nicht gilt, sollten die betroffenen

[11] Nach Artikel 4 Absatz 2 gelten Daten als unverständlich, wenn

a) sie auf sichere Weise mit einem Standardalgorithmus verschlüsselt worden sind, der zur Entschlüsselung verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zur Entschlüsselung verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann, oder

b) sie durch ihren mit einer kryptografischen verschlüsselten Standard-Hash-Funktion berechneten Hash-Wert ersetzt worden sind, der zum Daten-Hashing verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zum Daten-Hashing verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann.

Kunden benachrichtigt werden. Die Benachrichtigung sollte die klare Empfehlung enthalten, das durch die Sicherheitsverletzung beeinträchtigte Passwort in allen Konten, in denen es benutzt wird, zu ändern. In jedem Fall sollten die Benutzer bei der Anmeldung zum Online-Dienst gezwungen werden, ihr Passwort – unter Verwendung einer sicheren Methode – zu ändern.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Wenn die Passwörter sicher gespeichert worden wären (unter Verwendung einer dem Stand der Technik entsprechenden kryptografischen Hash-Funktion und eines Schlüssels oder zufälligen Salt-Werts), hätte dies die negativen Auswirkungen für die Betroffenen erheblich verringert. Personen mit schlecht gewählten Passwörtern können trotz solcher Maßnahmen weiterhin gefährdet sein, insbesondere dann, wenn sie dieselben Zugangsdaten für verschiedene Online-Dienste verwenden.

Fall 7: *Ein Internetdienstanbieter bietet Teilnehmern die Möglichkeit, ihre Konto- und Internetnutzungsdaten einzusehen; dies schließt Informationen über die monatliche Bandbreite und häufig besuchte Domains ein. Ein Kodierungsfehler auf der Website führt dazu, dass die Zugangsdaten der Benutzer nicht validiert werden und unbefugt auf Daten zugegriffen werden kann, indem der Wert der Teilnehmerkennung in den URL-Parametern verändert wird. Durch systematische Eingabe der aufeinander folgenden Teilnehmerkennungen kann auf die Kontodaten aller Kunden zugegriffen werden.*

Mögliche negative Folgen, die sich aus der Verletzung der Vertraulichkeit ergeben können:

- Die Daten können dazu benutzt werden, die betroffenen Personen per E-Mail oder telefonisch mit unerwünschter Werbung zu belästigen (Spamming).
- Die Daten können dazu benutzt werden, ein Profil des Teilnehmers zu erstellen. Da sie detaillierten Einblick in sein Verhalten bieten, können sie sensible Informationen enthalten. Die betroffenen Personen können in ihrem beruflichen und/oder familiären Umfeld beeinträchtigt werden.

Da anzunehmen ist, dass die betroffenen Personen durch diese Verletzung beeinträchtigt werden, sollten sie benachrichtigt werden.

Beispiele für geeignete Sicherheitsvorkehrungen, die im Fall ihrer rechtzeitigen Anwendung die Risiken hätten verringern können:

- Eine Überwachung der verwendeten Technologien auf mögliche Schwachstellen, wie in Fall 2 beschrieben, hätte die Verletzung möglicherweise verhindern können. Dies gilt ebenso für die Durchführung von Tests auf einer Probeplattform vor der Inbetriebnahme und die Überprüfung des Programmcodes.

3. Mögliche Szenarien, in denen eine Benachrichtigung der betroffenen Personen nicht erforderlich ist

Die Auswirkungen einer Verletzung des Schutzes personenbezogener Daten müssen auf Einzelfallbasis geprüft werden, damit alle Elemente einer möglichen Beeinträchtigung der betroffenen Personen angemessen berücksichtigt werden. Als allgemeine Richtschnur und ergänzend zu den im vorigen Abschnitt beschriebenen Ausnahmen kann der für die Verarbeitung Verantwortliche jedoch in bestimmten Fällen in Betracht ziehen, dass eine Benachrichtigung der betroffenen Personen nicht erforderlich ist.

Dazu gehören unter anderem folgende Fälle:

- Eine ausschließlich die Vertraulichkeit betreffende Verletzung personenbezogener Daten, wenn die Daten auf sichere Weise mit einem Standardalgorithmus verschlüsselt worden sind, der zur Entschlüsselung verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zur Entschlüsselung verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann. Solche Maßnahmen machen die Daten für alle Personen, die nicht zugriffsberechtigt sind, unverständlich.

- Die betroffenen Daten, wie etwa Passwörter, wurden unter Verwendung einer Hash-Funktion und eines Salt-Werts sicher verschlüsselt. Der Hash-Wert wurde mit Hilfe einer dem Stand der Technik entsprechenden kryptografischen verschlüsselten Hash-Funktion berechnet, der zum Daten-Hashing verwendete Schlüssel wurde durch keine Sicherheitsverletzung beeinträchtigt und der zum Daten-Hashing verwendete Schlüssel wurde so generiert, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann.

4. Fragen und Antworten

Wann kann die Benachrichtigung der betroffenen Personen unterbleiben?

- Immer wenn es sich bei der Sicherheitsverletzung nicht um eine Verletzung des Schutzes personenbezogener Daten handelt (siehe nächste Frage).
- Immer wenn nach einer Prüfung des Schweregrads der Verletzung davon auszugehen ist, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person durch die Verletzung nicht beeinträchtigt ist. Dies muss der zuständigen Behörde zu ihrer Zufriedenheit nachgewiesen werden.
- Immer wenn der Dienstanbieter zur Zufriedenheit der zuständigen Behörde nachgewiesen hat, dass er angemessene technische Schutzvorkehrungen getroffen hat und diese Schutzvorkehrungen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Dies trifft zum Beispiel zu, wenn bei einer ausschließlich die Vertraulichkeit betreffenden Verletzung des Schutzes personenbezogener Daten nur solche Daten betroffen sind, die entweder mit Hilfe eines dem Stand der Technik entsprechenden Algorithmus oder unter Verwendung eines Salt-Werts und einer dem Stand der Technik entsprechenden Hash-Funktion verschlüsselt wurden und bei denen die verwendeten geheimen Schlüssel und Salt-Werte durch keine Sicherheitsverletzung beeinträchtigt sind.
- Die Meldung von Verletzungen des Schutzes personenbezogener Daten, wie sie in dieser Stellungnahme beschrieben ist, stellt ein bewährtes Verfahren dar, das von allen für die Verarbeitung von Daten Verantwortlichen angewendet werden kann, auch wenn sie nicht obligatorisch ist.

Wann stellt eine Sicherheitsverletzung eine Verletzung des Schutzes personenbezogener Daten dar?

Eine Sicherheitsverletzung ist eine Verletzung des Schutzes personenbezogener Daten, wenn die von der Verletzung betroffenen Daten personenbezogene Daten im Sinne der Richtlinie 95/46/EG Artikel 2 Buchstabe a) sind: *alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.*

In der Stellungnahme 4/2007 wird ausgeführt, dass bei einer solcher Verletzung Daten betroffen sind, die sich auf eine Person beziehen: „eine Person [kann] direkt durch ihren Namen oder indirekt durch eine Telefonnummer, ein Autokennzeichen, eine Sozialversicherungsnummer, eine Reisepassnummer oder durch eine Kombination wesentlicher Kriterien identifiziert werden [...], die durch Eingrenzung der Gruppe (Alter, Beruf, Wohnort usw.), zu der die Person gehört, ihre Wiedererkennung ermöglichen." Weitere Erläuterungen zu dieser Frage finden sich in der Stellungnahme 4/2007.

Sollten die wahrscheinlichen sekundären Auswirkungen berücksichtigt werden?

Ja. Eine Verletzung des Schutzes personenbezogener Daten sollte den betroffenen Personen gemeldet werden, wenn anzunehmen ist, dass sie sich nachteilig auf die personenbezogenen Daten oder die Privatsphäre der Personen auswirkt.

Es sollten daher alle etwaigen Auswirkungen auf die betroffenen Personen in Betracht gezogen werden.

> ***Beispiel 1:*** *Die Website eines in der Musikbranche tätigen Unternehmens wurde Opfer eines Hackerangriffs. Die Benutzerdatenbank wurde gestohlen und im Internet veröffentlicht. Die entwendeten personenbezogenen Daten umfassen Namen/Familiennamen, Musikgeschmack sowie Benutzernamen und Passwörter der auf der Website des Unternehmens angemeldeten Benutzer. 9000 Benutzer sind betroffen.*

Bei dieser Verletzung mögen die direkten negativen Auswirkungen auf die betroffenen Personen in den meisten Fällen begrenzt erscheinen (Offenlegung von Informationen über den Musikgeschmack). Es kann sich daher die Frage stellen, ob die Benachrichtigung der betroffenen Personen unterbleiben kann. Da durch die Verletzung jedoch die Sicherheit der Passwörter beeinträchtigt wurde, müssen sie von dem für die Datenverarbeitung Verantwortlichen erneuert werden. Im Rahmen dieses Vorgangs ist es erforderlich, die Benutzer über die Gründe für die Erneuerung des Passworts zu informieren. Da außerdem viele Benutzer dasselbe Passwort für verschiedene Online-Konten verwenden[12], ist anzunehmen, dass als sekundäre Folge dieser Verletzung die Vertraulichkeit weiterer Konten beeinträchtigt wird. Die betroffenen Personen können diese sekundären Auswirkungen dadurch minimieren, dass sie die Passwörter aller ihrer Konten ändern. In der Benachrichtigung sollte deshalb auch auf die mögliche Beeinträchtigung anderer Konten hingewiesen und den betroffenen Personen empfohlen werden, für verschiedene Websites verschiedene Passwörter zu verwenden und das in seiner Sicherheit beeinträchtigte Passwort in allen Konten, in denen es benutzt wurde, zu ändern.

> ***Beispiel 2:*** *Das zweite Beispiel betrifft eine CD, die in einem Strafverfahren gegen eine Person als Beweismittel dienen kann. Die CD wurde per Einschreiben an einen Rechtsanwalt geschickt, ging jedoch in der Post verloren.*

Als unmittelbare Folge des Verlusts der CD ist die Datenverfügbarkeit beeinträchtigt. Die Auswirkungen auf den/die Betroffenen können vernachlässigbar oder gravierend sein, je nachdem, ob rechtzeitig geeignete Maßnahmen ergriffen werden können oder nicht.
Sekundäre Auswirkungen sind anzunehmen, wenn die CD ohne angemessenen Schutz verschickt wurde und Unbefugte Zugang zu den Daten erhalten. In diesem Fall könnte die unbefugte Person die Daten lesen, sie an Journalisten verkaufen usw., was den/die Betroffenen sehr stark beeinträchtigen dürfte.

In diesem Beispiel wären die direkten Auswirkungen auf die betroffene Person vernachlässigbar, wenn die CD rechtzeitig erneut zugestellt werden kann, so dass eine Benachrichtigung unterbleiben könnte. Die sekundären Auswirkungen der Verletzung sind dagegen als sehr hoch einzuschätzen und machen es auf jeden Fall erforderlich, die Betroffenen zu informieren.

Muss eine Benachrichtigung erfolgen, auch wenn es sich nur um eine betroffene Person handelt?

[12] Jüngeren Studien zufolge verwenden 55-80 % der Internet-Benutzer ein- und dasselbe Passwort für verschiedene Konten.

Ja. Die Meldung einer Verletzung des Schutzes personenbezogener Daten wird in der Richtlinie 2002/58/EG nicht davon abhängig gemacht, dass eine bestimmte Mindestanzahl von Personen betroffen ist. In der Verordnung (EU) Nr. 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG heißt es dazu in Artikel 3 Absatz 1: „Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten die personenbezogenen Daten eines Teilnehmers oder einer Person oder deren Privatsphäre beeinträchtigt werden, so benachrichtigt der Betreiber zusätzlich zu der Benachrichtigung gemäß Artikel 2 auch den Teilnehmer bzw. die Person von der Verletzung."

Der für die Verarbeitung Verantwortliche sollte also eine Verletzung unabhängig von der Zahl der betroffenen Personen immer dann melden, wenn negative Auswirkungen anzunehmen sind.

Wie ist mit Daten umzugehen, die wahrscheinlich öffentlich sind?

Zwei Aspekte sollten berücksichtigt werden.

1. Mit dem Begriff „öffentlich" können verschiedene Ebenen der Verfügbarkeit bezeichnet werden: Daten können über das Internet frei zugänglich sein, sie können im Rahmen eines Abonnementdienstes öffentlich zugänglich sein oder sie stehen offline auf Anfrage öffentlich zur Verfügung.
   In Frankreich zum Beispiel wird bei Wahlen das Wählerverzeichnis im Rathaus ausgehängt. Jeder Wähler und jede politische Partei kann Einsicht nehmen, doch ist es gesetzlich verboten, diese Listen online zu veröffentlichen.
   Die versehentliche Versendung einer elektronischen Fassung des Verzeichnisses an den falschen Wähler oder der Verlust einer Papierversion der Liste stellen somit keine Verletzung der Vertraulichkeit der Daten dar, während die Veröffentlichung des Verzeichnisses im Internet die Vertraulichkeit verletzen würde und gemeldet werden müsste.

2. Bestimmte Daten können für einige Personen öffentlich sein, für andere nicht.
   So kann eine mit einem Nachnamen verknüpfte Liste von Telefonnummern sowohl öffentlich in Telefonbüchern verfügbare Telefonnummern als auch Geheimnummern enthalten.

Zusammenfassend lässt sich feststellen, dass eine Verletzung der Vertraulichkeit von Daten immer dann vorliegt, wenn die Ebene, auf der die Daten zur Verfügung stehen, geändert wurde. Eine solche Verletzung sollte also (sofern von einer Beeinträchtigung der betroffenen Personen auszugehen ist) gemeldet werden.

Wie soll die Benachrichtigung erfolgen, wenn die Kontaktdaten der betroffenen Personen unvollständig oder unbekannt sind?

Es gibt Fälle, in denen der Dienstanbieter, selbst wenn er in einem direkten Vertragsverhältnis zum Endnutzer steht, nicht über genügend Angaben verfügt, um die betroffenen Personen ordnungsgemäß zu benachrichtigen. Auch wenn in diesem Fall die Möglichkeit in Betracht gezogen werden kann, die Betroffenen durch Bekanntmachungen in den Medien zu

benachrichtigen, besteht gleichwohl die Verpflichtung fort, alle zumutbaren Anstrengungen zu unternehmen, um die Betroffenen persönlich zu benachrichtigen.[13]

Obwohl die Verpflichtung, weiterhin alle zumutbaren Anstrengungen zu unternehmen, dem jeweils betroffenen Dienstanbieter obliegt und er alle vertretbaren Maßnahmen ergreifen soll, um sicherzustellen, dass alle betroffenen Personen von der Verletzung in Kenntnis gesetzt werden, schließt dies gleichwohl nicht die Möglichkeit aus, dass er andere Dienstanbieter oder für die Verarbeitung von Daten Verantwortliche, die im Besitz der Kontaktdaten sind, um Unterstützung bittet. Im oben beschriebenen Fall 4 könnte also der für die Verarbeitung Verantwortliche, wenn er nicht über die Kontaktdaten der betroffenen Karteninhaber verfügt, den zwischengeschalteten Zahlungsverkehrsdienstleister benachrichtigen, der die betroffenen Personen leicht kontaktieren kann. In anderen Fällen kann es notwendig sein, mit den zuständigen Behörden zusammenzuarbeiten. Diese müssen auf jeden Fall informiert werden, wenn der Dienstanbieter die Benachrichtigung der betroffenen Personen nicht sicherstellen kann.

Ist es notwendig, Personen zu benachrichtigen, die von der Verletzung des Schutzes personenbezogener Daten nicht betroffen wurden?

Nein, solche Personen müssen nicht benachrichtigt werden, sofern zuverlässig festgestellt werden kann, dass sie nicht von der Datenschutzverletzung betroffen sind. Kann zum Beispiel nachgewiesen werden, dass eine Teilmenge der betroffenen Personen nicht von der Sicherheitsverletzung betroffen wurde, brauchen diese Betroffenen nicht benachrichtigt zu werden. Die für die Datenverarbeitung Verantwortlichen müssen jedoch bei ihrer Entscheidung alle wahrscheinlichen negativen Auswirkungen in Betracht ziehen. Je nach Art der Sicherheitsverletzung kann es die betroffenen Personen auch beunruhigen, keine Benachrichtigung zu erhalten.

[13] Gemäß Artikel 3 Absatz 7 der Verordnung (EU) Nr. 611/2013 kann der Betreiber, wenn er trotz aller zumutbaren Anstrengungen nicht alle Personen ermitteln kann, die von der Verletzung des Schutzes personenbezogener Daten wahrscheinlich beeinträchtigt werden, diese innerhalb der geltenden Frist durch Bekanntmachungen in großen nationalen oder regionalen Medien der betreffenden Mitgliedstaaten benachrichtigen. Dessen ungeachtet ist er nach dem Artikel verpflichtet, weiterhin alle zumutbaren Anstrengungen zu unternehmen, um diese Personen zu ermitteln und sie so bald wie möglich zu benachrichtigen.