Juristische Rahmenbedingungen für den Umgang mit Data Leakage

Dr. Martin Braun
Rechtsanwalt

GI-Fachgruppe Management von Informationssicherheit
Frankfurt am Main, 25. Februar 2011

WILMERHALE
WILMER CUTLER PICKERING HALE AND DORR LLP

Übersicht

- Allgemeiner Rechtsrahmen, präventive Pflichten
  - Strafrecht
  - Vertragsrecht
  - Datenschutzrecht
- Reaktionsmöglichkeiten und –pflichten
  - Hintergrund: Entwicklung in den USA
  - § 42a BDSG
  - RL 2002/58/EG

Allgemeiner Rechtsrahmen, präventive Pflichten

Zum Begriff „Data Leakage“

Wikipedia (Stichwort: Data Loss Prevention):

„Data Loss Prevention“ = Schutz gegen den unerwünschten Abfluss von Daten, der Schaden versursacht und auch bemerkt wird

„Data Leakage Prevention“ = Schutz gegen ein vermutetes, aber nicht messbares und manchmal im Einzelfall gar nicht feststellbares Weitergeben von Informationen an unerwünschte Empfänger

In der Regel aber synonymer Gebrauch

Strafrechtlicher Schutz von Geheimnissen

Anknüpfungspunkt: „Geheimnis“

- **§ 17 UWG** (Verrat von Geschäfts- und Betriebsgeheimnissen)
- **§ 353b StGB** (Verletzung von Dienstgeheimnissen oder besonderen Geheimhaltungspflichten)
- **§ 203 StGB** (Verletzung von Privatgeheimnissen)
- **§§ 93-97b StGB** (Schutz von Staatsgeheimnissen)

Literatur:
Wissenschaftliche Dienste des Deutschen Bundestages, „Aktueller Begriff – Der strafrechtliche Schutz von Geheimnissen“ (Dez 2010)

Vertragliche Regelungen

Anknüpfungspunkt: Parteiwille

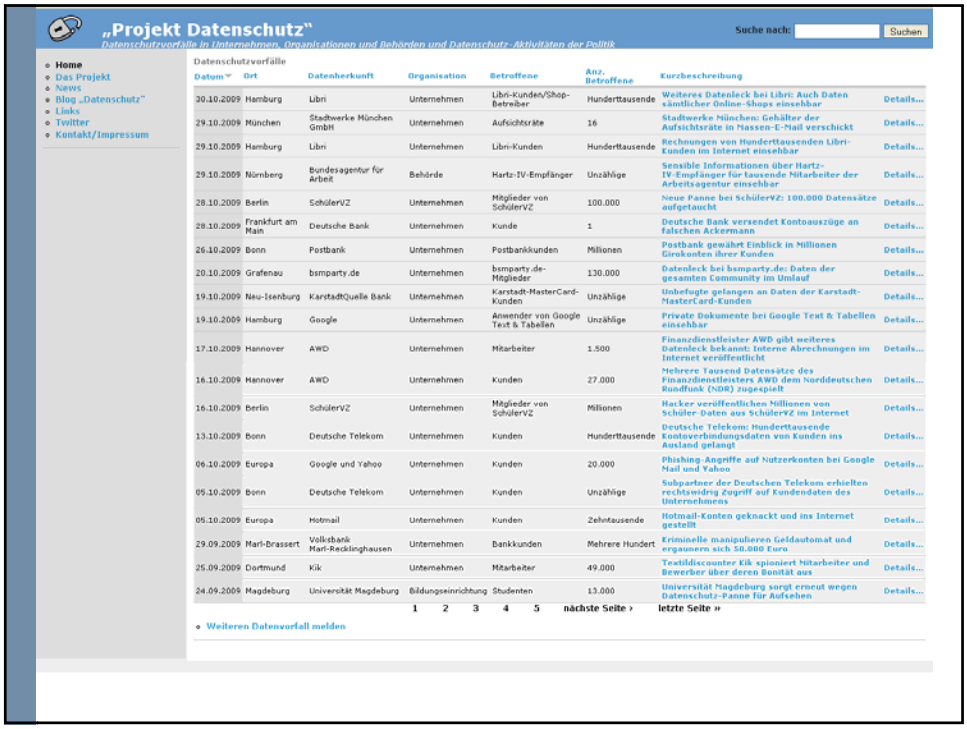
- Gesonderte Vertraulichkeitsvereinbarungen
- Vertraulichkeitsregelungen im Vertrag
- Pro und Contra Vertragsstrafe
- Schadensersatzregelungen

Bundesdatenschutzgesetz

Anknüpfungspunkt: „personenbezogene Daten“

- Grundsatz: Verbot mit Erlaubnisvorbehalt
- Datensparsamkeit
- Technische und organisatorische Schutzmaßnahmen, § 9 BDSG und Anlage
- Datengeheimnis, § 5 BDSG
- Seit 2009 verschärfte Anforderungen im Bereich Auftragsdatenverarbeitung, § 11 BDSG
- Zusätzliche Beschränkung von Übermittlungen in das Ausland

Reaktionsmöglichkeiten und -pflichten



„Projekt Datenschutz"

Datenschutzvorfälle in Unternehmen, Organisationen und Behörden und Datenschutz-Aktivitäten der Politik

Suche nach: Suchen

- Home
- Das Projekt
- News
- Blog „Datenschutz"
- Links
- Twitter
- Kontakt/Impressum

Datenschutzvorfälle

Datum	Ort	Datenherkunft	Organisation	Betroffene	Anz. Betroffene	Kurzbeschreibung	
30.10.2009	Hamburg	Libri	Unternehmen	Libri-Kunden/Shop-Betreiber	Hunderttausende	Weiteres Datenleck bei Libri: Auch Daten sämtlicher Online-Shops einsehbar	Details...
29.10.2009	München	Stadtwerke München GmbH	Unternehmen	Aufsichtsräte	16	Stadtwerke München: Gehälter der Aufsichtsräte in Massen-E-Mail verschickt	Details...
29.10.2009	Hamburg	Libri	Unternehmen	Libri-Kunden	Hunderttausende	Rechnungen von Hunderttausenden Libri-Kunden im Internet einsehbar	Details...
29.10.2009	Nürnberg	Bundesagentur für Arbeit	Behörde	Hartz-IV-Empfänger	Unzählige	Sensible Informationen über Hartz-IV-Empfänger für tausende Mitarbeiter der Arbeitsagentur einsehbar	Details...
28.10.2009	Berlin	SchülerVZ	Unternehmen	Mitglieder von SchülerVZ	100.000	Neue Panne bei SchülerVZ: 100.000 Datensätze aufgetaucht	Details...
28.10.2009	Frankfurt am Main	Deutsche Bank	Unternehmen	Kunde	1	Deutsche Bank versendet Kontoauszüge an falschen Ackermann	Details...
26.10.2009	Bonn	Postbank	Unternehmen	Postbankkunden	Millionen	Postbank gewährt Einblick in Millionen Girokonten ihrer Kunden	Details...
20.10.2009	Grafenau	bsmparty.de	Unternehmen	bsmparty.de-Mitglieder	130.000	Datenleck bei bsmparty.de: Daten der gesamten Community im Umlauf	Details...
19.10.2009	Neu-Isenburg	KarstadtQuelle Bank	Unternehmen	Karstadt-MasterCard-Kunden	Unzählige	Unbefugte gelangen an Daten der Karstadt-MasterCard-Kunden	Details...
19.10.2009	Hamburg	Google	Unternehmen	Anwender von Google Text & Tabellen	Unzählige	Private Dokumente bei Google Text & Tabellen einsehbar	Details...
17.10.2009	Hannover	AWD	Unternehmen	Mitarbeiter	1.500	Finanzdienstleister AWD gibt weiteres Datenleck bekannt: Interne Abrechnungen im Internet veröffentlicht	Details...
16.10.2009	Hannover	AWD	Unternehmen	Kunden	27.000	Mehrere Tausend Datensätze des Finanzdienstleisters AWD dem Norddeutschen Rundfunk (NDR) zugespielt	Details...
16.10.2009	Berlin	SchülerVZ	Unternehmen	Mitglieder von SchülerVZ	Millionen	Hacker veröffentlichen Millionen von Schüler-Daten aus SchülerVZ im Internet	Details...
13.10.2009	Bonn	Deutsche Telekom	Unternehmen	Kunden	Hunderttausende	Deutsche Telekom: Hunderttausende Kontoverbindungsdaten von Kunden ins Ausland gelangt	Details...
06.10.2009	Europa	Google und Yahoo	Unternehmen	Kunden	20.000	Phishing-Angriffe auf Nutzerkonten bei Google Mail und Yahoo	Details...
05.10.2009	Bonn	Deutsche Telekom	Unternehmen	Kunden	Unzählige	Subpartner der Deutschen Telekom erhielten rechtswidrig Zugriff auf Kundendaten des Unternehmens	Details...
05.10.2009	Europa	Hotmail	Unternehmen	Kunden	Zehntausende	Hotmail-Konten geknackt und ins Internet gestellt	Details...
29.09.2009	Marl-Brassert	Volksbank Marl-Recklinghausen	Unternehmen	Bankkunden	Mehrere Hundert	Kriminelle manipulieren Geldautomat und ergaunern sich 50.000 Euro	Details...
25.09.2009	Dortmund	Kik	Unternehmen	Mitarbeiter	49.000	Textildiscounter Kik spioniert Mitarbeiter und Bewerber über deren Bonität aus	Details...
24.09.2009	Magdeburg	Universität Magdeburg	Bildungseinrichtung	Studenten	13.000	Universität Magdeburg sorgt erneut wegen Datenschutz-Panne für Aufsehen	Details...

1 2 3 4 5 nächste Seite › letzte Seite »

- Weiteren Datenvorfall melden

A Chronology of Data Breaches

Posted April 20, 2005
Updated October 30, 2009

Privacy Rights CLEARINGHOUSE

Search Our Site:
www.privacyrights.org/search/search.php
Have a Question?
www.privacyrights.org/preinquiry.htm
Web: www.privacyrights.org

HOME

A Chronology of Data Breaches

Printing tip: Use the "landscape" setting for best results when printing the breach list.

Skip the introductory text and go directly to the listing of data breaches below.

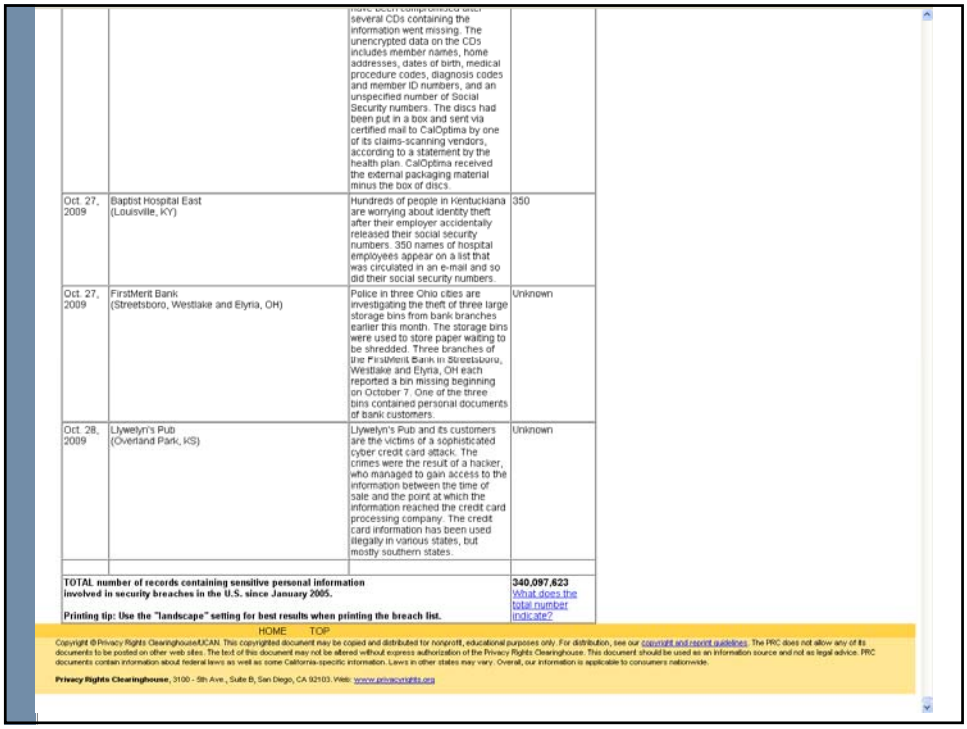
- What does the Chronology of Data Breaches contain?
- What does the Total Number indicate?
- Is the Chronology of Data Breaches a complete listing of all breaches?
- Are there state-specific breach listings?
- How often is the Chronology updated?
- Where do you obtain information about the data breaches that are reported on this Web page?
- What should I do if my personal information has been compromised in a data breach?
- Are there resources for businesses and other organizations on how to avoid having sensitive data breached?
- What should I do if my business or organization experiences a security breach?
- Do states have laws that require those entities that experience a data breach to notify the affected individuals?
- Which states have laws that require breached organizations to report breaches and submit notice letters to a central clearinghouse?
- Has anyone analyzed this and other data breach listings in order to compile statistics and arrive at other observations? Have any analyses of security breach laws been published?
- Are there other resources with additional information about security breaches?
- Go directly to the listing of data breaches

What does the Chronology of Data Breaches contain?

The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. Some breaches that do NOT expose such sensitive information have been included in order to underscore the variety and frequency of data breaches. However, we have not included the number of records involved in such breaches in the total because we want this compilation to reflect breaches that expose individuals to identity theft as well as breaches that qualify for disclosure under state laws. *The breaches posted below include only those reported in the United States. They do **not** include incidents in other countries.*

What does the Total Number indicate?

The running total we maintain at the end of the Chronology represents the approximate number of "records" that have



		several CDs containing the information went missing. The unencrypted data on the CDs includes member names, home addresses, dates of birth, medical procedure codes, diagnosis codes and member ID numbers, and an unspecified number of Social Security numbers. The discs had been put in a box and sent via certified mail to CalOptima by one of its claims-scanning vendors, according to a statement by the health plan. CalOptima received the external packaging material minus the box of discs.	
Oct. 27, 2009	Baptist Hospital East (Louisville, KY)	Hundreds of people in Kentuckiana are worrying about identity theft after their employer accidentally released their social security numbers. 350 names of hospital employees appear on a list that was circulated in an e-mail and so did their social security numbers.	350
Oct. 27, 2009	FirstMerit Bank (Streetsboro, Westlake and Elyria, OH)	Police in three Ohio cities are investigating the theft of three large storage bins from bank branches earlier this month. The storage bins were used to store paper waiting to be shredded. Three branches of the FirstMerit Bank in Streetsboro, Westlake and Elyria, OH each reported a bin missing beginning on October 7. One of the three bins contained personal documents of bank customers.	Unknown
Oct. 28, 2009	Llywelyn's Pub (Overland Park, KS)	Llywelyn's Pub and its customers are the victims of a sophisticated cyber credit card attack. The crimes were the result of a hacker, who managed to gain access to the information between the time of sale and the point at which the information reached the credit card processing company. The credit card information has been used illegally in various states, but mostly southern states.	Unknown
TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005. **Printing tip: Use the "landscape" setting for best results when printing the breach list.**			**340,097,623** What does the total number indicate?

HOME TOP

Privacy Rights Clearinghouse, 3100 - 5th Ave., Suite B, San Diego, CA 92103. Web: www.privacyrights.org

Rechtliche Entwicklung in den USA (Überblick)

- Ebene der Einzelstaaten (seit 2002)
- Bundesebene
  - Spezialgesetze
  - Initiativen zur Vereinheitlichung
- Kosten, „Credit Rating“ u.a.
- Class Action

Relevanz für deutsche Unternehmen?

§ 42a BDSG

- Eine Stelle nach § 2 Abs. 4 oder § 27 Abs. 1 S. 1 BDSG stellt fest, dass
- bei ihr gespeicherte
  - sensitive Daten (§ 3 Abs. 9 BDSG),
  - personenbezogene Daten, die Berufsgeheimnis unterliegen,
  - personenbezogene Daten, die sich auf strafbare Handlungen, OWi oder deren Verdacht beziehen, oder
  - personenbezogene Daten zu Bank- oder Kreditkartenkonten

§ 42a BDSG (II)

- unrechtmäßig übermittelt *oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind*, und
- es drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des Betroffenen

§ 42a BDSG – Inhalt (Konsequenzen)

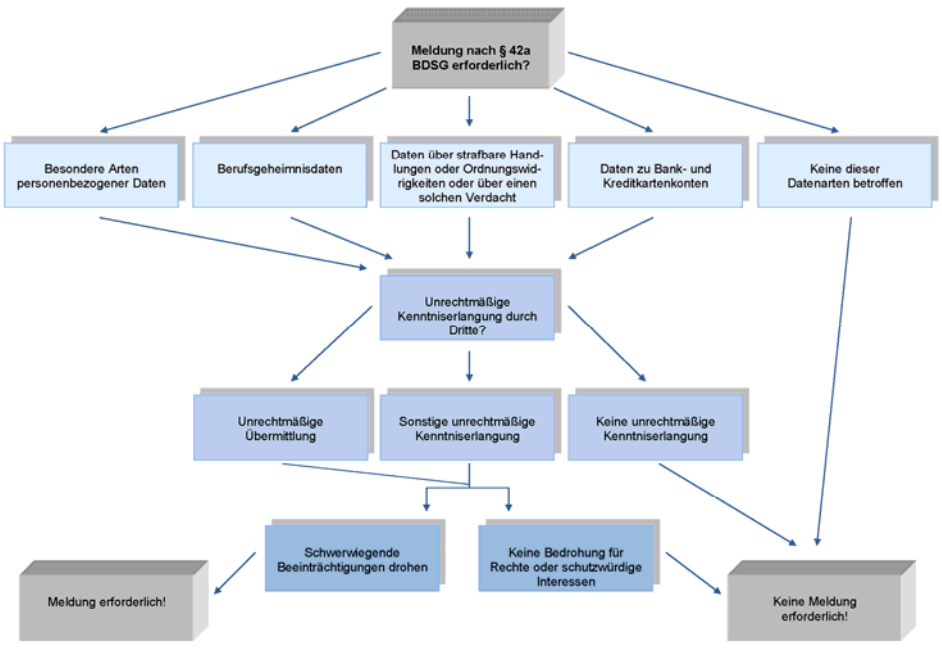
- Pflicht zur Benachrichtigung des Betroffenen:
  - Unverzüglich, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird.
  - Muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten.

§ 42a BDSG – Inhalt (Konsequenzen)

- Bei unverhältnismäßigem Aufwand für die Benachrichtigung: Information der Öffentlichkeit durch Anzeige in zwei bundesweit erscheinenden Tageszeitungen (mindestens eine halbe Seite) oder vergleichbare Maßnahme.

§ 42a BDSG – Inhalt (Konsequenzen)

- Benachrichtigung der Aufsichtsbehörde
  - unverzüglich
  - Inhalt wie gegenüber dem Betroffenem
  - Zusätzlich: Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen



Quelle: Berliner Beauftragter für Datenschutz und Informationsfreiheit
http://www.datenschutz-berlin.de/attachments/730/535-4-3.pdf?1292856596

§ 42a BDSG – Inhalt (Beweisverwertungsverbot)

- Benachrichtigung darf in Straf- und OWiG-Verfahren nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden

§§ 42a, § 43 Abs. 2 Nr. 7 BDSG

- OWi-Tatbestand,
- bis zu EUR 300.000 Geldbuße
- wenn Mitteilung vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgt

§ 93 Abs. 3 TKG, § 15a TMG

- Vergleichbare Regelungen für Anbieter von Telekommunikationsdiensten und Telemediendiensten
- Keine eigene Bußgeldregelung

Weitere Themen

- Wer ist bei Auftragsdatenverarbeitung zur Meldung verpflichtet?
- Umsetzung im Unternehmen

- Unterlassungsansprüche § 1004 BGB
- Schadensersatz
- Einschaltung der Staatsanwaltschaft

Entwicklung in der Europäischen Union

- Änderung der Richtlinie 2002/58/EG im Dezember 2009
- Gesetzgebungsverfahren zur Umsetzung in Deutschland läuft
- Verfahren zur Änderung der Richtlinie 95/46/EG ist angestoßen

Entwicklung in der Europäischen Union

Neue Definition in Art. 2(i)

- „Verletzung des Schutzes personenbezogener Daten“ eine 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.“

Neufassung RL 2002/58/EG, Art. 4

Artikel 4 (Sicherheit der Verarbeitung)

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

Neufassung RL 2002/58/EG, Art. 4

1a) Unbeschadet der Richtlinie 95/46/EG ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen:

- Sicherstellung, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten,
- Schutz gespeicherter oder übermittelter personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust oder unbeabsichtigter Veränderung und unbefugter oder unrechtmäßiger Speicherung oder Verarbeitung, unbefugtem oder unberechtigtem Zugang oder unbefugter oder unrechtmäßiger Weitergabe

und

- Sicherstellung der Umsetzung eines Sicherheitskonzepts für die Verarbeitung personenbezogener Daten.

Neufassung RL 2002/58/EG, Art. 4

(3) Im Fall einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste unverzüglich die zuständige nationale Behörde von der Verletzung.

Neufassung RL 2002/58/EG, Art. 4

Ist anzunehmen, dass durch die Verletzung personenbezogener Daten die personenbezogenen Daten, oder Teilnehmer oder Personen in ihrer Privatsphäre, beeinträchtigt werden, so benachrichtigt der Betreiber auch den Teilnehmer bzw. die Person unverzüglich von der Verletzung.

Der Anbieter braucht die betroffenen Teilnehmer oder Personen nicht von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn er zur Zufriedenheit der zuständigen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. Diese technischen Schutzmaßnahmen verschlüsseln die Daten für alle Personen, die nicht befugt sind, Zugang zu den Daten zu haben.

Neufassung RL 2002/58/EG, Art. 4

[…] kann die zuständige nationale Behörde, wenn der Betreiber den Teilnehmer bzw. die Person noch nicht über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, diesen nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung zur Benachrichtigung auffordern.

In der Benachrichtigung des Teilnehmers bzw. der Person werden mindestens die Art der Verletzung des Schutzes personenbezogener Daten und die Kontaktstellen, bei denen weitere Informationen erhältlich sind, genannt und Maßnahmen zur Begrenzung der möglichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten empfohlen. In der Benachrichtigung der zuständigen nationalen Behörde werden zusätzlich die Folgen der Verletzung des Schutzes personenbezogener Daten und die vom Betreiber nach der Verletzung vorgeschlagenen oder ergriffenen Maßnahmen dargelegt.

Literatur

- Berliner Beauftragter für Datenschutz und Informationsfreiheit: FAQs zur Informationspflicht bei § 42a BDSG (Stand Dezember 2010)

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Martin Braun
martin.braun@wilmerhale.com

Ulmenstraße 37-39
60325 Frankfurt am Main
Tel. +49 (69) 27 10 78 000
Fax. +49 (69) 27 10 78 100