5 Einbruch in die Geschäftsräume

Thomas Jäschke und Christine Thieme

5.1 Datenschutz-Aspekte bei Einbrüchen

Bei einem Einbruch in Geschäftsräume werden die wenigsten zuerst an einen damit verbundenen Datenschutzvorfall denken. Im Fokus der meisten Einbrecher stehen sicherlich auch in erster Linie schnell verwertbares Diebesgut wie Bargeld oder Betäubungsmittel. Werden – und das ist nicht selten – auch Festrechner und Mobilgeräte gestohlen, muss bei der Schadensbeseitigung auch bedacht werden, dass auf diesen Geräten personenbezogene Daten gespeichert sind. Dies gilt auch bei einem Diebstahl von medizinischen Geräten. Je nach Bauart muss damit gerechnet werden, dass auf diesen personenbezogene Daten gespeichert wurden. Bei diesen Daten, zu denen ein Einbrecher auf diesen Weg Zugriff erhält, handelt es sich fast immer um sensible Daten im Sinne von § 3 Abs. 9 BDSG. Eine Fernsehsendung der ARD demonstrierte im Oktober 2015 welche Daten der Festplatte eines Kopierers herausgelesen werden können. In diesen Fällen standen die Kopierer zuvor in den Büros von Rechtsanwälten (vgl. ARD 2015, Sendung Plusminus). Insofern ist der Einbruch in Geschäftsräume nicht nur ein äußerst unerfreuliches Ereignis, welches eine Anzeige bei der Polizei sowie eine Meldung an die Versicherung erfordert. Steht zu befürchten, dass mit dem Diebstahl von IT- und Medizingeräten auch der Verlust von personenbezogenen Daten einhergeht, so ist die verantwortliche Stelle gemäß § 42a BDSG verpflichtet, den Betroffenen und die zuständige Aufsichtsbehörde zu informieren:

„Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. *besondere Arten personenbezogener Daten (§ 3 Absatz 9),*
2. *personenbezogene Daten, die einem Berufsgeheimnis unterliegen*
3. *personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder*
4. *personenbezogene Daten zu Bank- oder Kreditkartenkonten*

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 sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen."

Dies bedeutet neben dem Aufwand auch – angesichts der Sensibilität der Daten – einen immensen Vertrauensverlust gegenüber den betroffenen Kunden und Patienten und unangenehme Nachfragen, ggf. auch Bußgelder der Aufsichtsbehörden.

Zwar lässt sich auch mit größtem Aufwand ein Einbruch nicht zu 100% verhindern, mit Sicherheitsmaßnahmen kann die Wahrscheinlichkeit allerdings deutlich gesenkt werden. Weiterhin sollte man für den Fall, dass ein Einbruch zu einem unberechtigten Zugriff auf personenbezogene Daten führt, einen Notfallplan entwickeln, der hilft, den entstandenen Schaden zu begrenzen. Der Schwerpunkte dieses Kapitels liegt auf den physischen Einbrüchen, wobei auch auf digitale Einbrüche eingegangen wird.

5.2 Präventivmaßnahmen

Als Hilfsmittel oder Checkliste für Präventivmaßnahmen können die technisch-organisatorischen Maßnahmen herangezogen werden. Diese technisch-organisatorischen Maßnahmen sind Maßgaben, die in § 9 BDSG und dem Anhang zu § 9 BDSG beschrieben werden. Datenverarbeitende Stellen sind verpflichtet, diese Maßnahmen einzuhalten, um so personenbezogene Daten, die bei ihnen verarbeitet werden, gegen unberechtigte Zugriffe, Zerstörung oder Verlust zu schützen (s.a. Kap. V.1). Technisch-organisatorische Maßnahmen sind nicht nur Maßnahmen der IT, z.B. die Installation von Virensoftware, das Einrichten komplexer Passwörter und Back-ups, sondern auch Maßnahmen zur Sicherung der Gebäude und Räumlichkeiten. In Bezug auf physische wie digitale Einbrüche spielen insbesondere Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle eine große Rolle. Eine gute Übersicht über die Maßnahmen gibt die Broschüre Datensicherheit des BayLDA. Auch in dem Muster zur Auftragsdatenverarbeitung des GDD findet man in den Hinweisen zur Erstellung einer Anlage nach § 11 BDSG (ab Seite 9) einen Fragebogen mit Maßnahmen, die man in Hinblick auf den Schutz seiner eigenen Geschäftsräume prüfen kann. Detailfreudiger ist das BSI, dass in seinen Maßnahmenkatalogen die Sicherung von Türen und Fenstern und Einbrüche in Geschäftsräumen in den Kapiteln M1 Infrastruktur regelt. Nachfolgend werden einige Beispiele genannt.

Zutrittskontrolle

Mit Zutrittskontrolle werden die Maßnahmen definiert, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren. Darunter können Maßnahmen fallen wie

- Sicherung der Zugänge durch Zäune, Pforte, Sicherheitsschlösser,
- Prüfung unvermuteter Zugänge wie Lichtschächte und Fenster,
- Sicherung von Rollos gegen Hochschieben, Sicherheitsverglasung,
- Videoüberwachung, Alarmanlagen sowie
- Einsatz eines Wachdienstes.

Neben technischen Maßnahmen spielen auch organisatorische Maßnahmen eine Rolle. Dazu gehört vor allem die Sensibilisierung der Mitarbeiter, die Türen und Fenster der Räume und Gebäude bei Verlassen – auch bei kurzfristiger Abwesenheit während der Mittagspause – immer zu verschließen. Angesichts der regelmäßigen Warnungen der Polizei, dass Einbrüchen oft ein Ausspionieren durch die Täter vorhergeht, sollten Mitarbeiter angewiesen werden, Besucher zu registrieren und sie im Gebäude zu begleiten. Mitarbeiter, die im Empfangsbereich arbeiten sollten auch explizit darüber aufgeklärt werden, dass sie den Zweck eines Besuches hinterfragen. Sind sie zum Beispiel nicht darüber aufgeklärt, dass ein Termin mit einem Handwerker oder mit IT-Servicepersonal vereinbart wurde, dann sollten sie diesen unangekündigten Besucher erst nach einer Rückversicherung bei dem Hausmeister oder bei den anderen Kollegen in die Räumlichkeiten lassen. Die anderen Mitarbeiter sollen ihre Kollegen aus dem Empfangsbereich dahingehend unterstützen, dass sie diese über Besucher informieren. Besucher sollten im Gebäude nach Möglichkeit immer einen Besucherausweis tragen, ihr Kommen und Gehen sollte in einer Liste (unter Wahrung des Prinzips der Datensparsamkeit und der Erforderlichkeit) registriert werden. Bei der Registrierung ist es erlaubt, sich den Personalausweis oder einen anderen Identifikationsnachweis vorzeigen zu lassen. Das pauschale Anfertigen von Kopien ist allerdings gemäß eines Urteil des VG Hannover (2013, Az. 10 A 534211) nicht erlaubt, da dies gegen das Gebot der Verhältnismäßigkeit verstößt.

Bei der Auswahl der geeigneten Maßnahmen beraten viele Polizeidienststellen, welche technischen und mechanischen Schutzvorkehrungen Sinn machen. So rät die Berliner Polizei Arztpraxen zur Montage von Türen und Fenstern der Widerstandsklasse 3 gemäß Euro-Norm DIN V ENV 1627 und zu Schlössern mit Bohrschutz sowie Schutzbeschläge und Zylinderabdeckungen (vgl. Gewerkschaft der Polizei 2015).

Bei aller Einbruchgefahr müssen allerdings auch die Maßgaben des BDSG bezüglich der „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischer Einrichtungen" (§ 6b BDSG) beachtet werden. Bei vielen Einrichtungen des Gesundheitswesens – Arztpraxen, Krankenhäusern etc. – handelt es sich um öffentlich zugängliche Räumlichkeiten, sodass die Installation von Videokameras nur zur Wahrnehmung des Hausrechtes bzw. berechtigter Interessen für konkret festgelegte Zwecke zulässig ist. Die Maßgaben, die nicht nur gegenüber den Besuchern, sondern auch gegenüber den Mitarbeitern aufgrund ihres schutzwürdigen Interesses einzuhalten sind, werden in Kapitel V.6 „Vorgehen Kameraüberwachung" detailliert erläutert.

Zugangskontrolle und Zugriffskontrolle

Die Maßnahmen, die in diesen Bereich fallen, betreffen mehr den Schutz der Daten gegen einen digitalen Einbruch, wobei dieser eine Folge des physischen Einbruchs sein kann, wenn z.B. aus der Praxis oder aus dem Auto Laptops oder Mobilgeräte entwendet werden. Ein physischer Einbruch kann auch durchaus in der Absicht durchgeführt werden, sich unberechtigten Zugang zu Daten zu verschaffen und mit diesen

digitalen einzubrechen. Beispielsweise können Rechnungsunterlagen, auf denen Kontoverbindungsdaten oder die E-Mail-Adressen von Patienten vermerkt sind, die Basis für Hackerangriffe darstellen.

Die Zugangskontrolle beschreibt dabei Maßnahmen, die verhindern, dass Unbefugte in die IT-Systeme eindringen. Maßnahmen zur Zugriffskontrolle gewährleisten, dass nur die zur Benutzung eines Systems Berechtigten im Rahmen ihrer Zugriffsberechtigungen auf Daten zugreifen können und diese lesen, kopieren oder verändern können. Dies können z.B. folgende Maßnahmen sein (vgl. BayLDA 2014, Checkliste Datensicherheit, S. 3–4):

- sichere Aufbewahrung von Geräten in verschlossenen Schränken
- Inventarisierung von Datenträgern, um infolge eines Einbruchs einen Abgleich machen zu können
- Benutzeridentifikation und Passwortrichtlinien, die komplexe Passwörter erfordern
- Systemsperrung nach mehrmaliger Fehleingabe
- Verschlüsselung von Geräten und Datenträgern

Bezüglich der Aufbewahrung von Daten in Papierform – gerade im Gesundheitsbereich werden viele sensible Daten noch immer in Papierform gespeichert – sollte eine Clean-Desk-Policy verfolgt werden, d.h. es sollten ohnehin möglichst wenig Akten oder Karteikarten auf den Schreibtischen liegen, und diese sollten bei Arbeitsende immer eingeschlossen werden. Die Schrankschlüssel müssen entsprechend sicher aufgehoben werden.

Weiterhin sollte als Präventivmaßnahme die Möglichkeit eingerichtet werden, sensible Daten bzw. die komplette Festplatte oder das mobile Gerät im Rahmen einer Fernwartungsoption unverzüglich zu löschen sobald ein Einbruch festgestellt worden ist. Voraussetzung hierfür ist in jedem Fall eine regelmäßige Datensicherung und eine Aufbewahrung der Daten an einem Ort, der sich außerhalb der Geschäftsräume befindet. Falls Geräte bei einem Einbruch entwendet werden, stellt dies sicher, dass die Daten, die auf dem Gerät per Fernwartung gelöscht werden, an einem anderen Ort zur Verfügung stehen. Abgesehen davon ist dies auch immer ein Schutz gegen zufällige oder beabsichtigte Zerstörung, die nie ausgeschlossen werden kann, z.B. wenn ein Einbruch mit Vandalismus seitens der Täter verbunden ist. Gegebenenfalls wird die Fernwartung über einen externen Dienstleister sichergestellt, z.B. wenn Geräte wie Kopierer geleast werden. Hier sollte z.B. mit dem Hersteller oder dem Dienstleister besprochen werden, wie Daten im Schadensfall gelöscht werden können.

Einschätzung der Daten nach Schutzbedarf und Inventarisierung

Bei Einführung der Maßnahmen sollte bedacht werden, dass die ergriffenen Maßnahmen in einem angemessenen Verhältnis zu ihrem Schutzbedarf stehen sollte. Wenn sehr umfangreiche Maßnahmen für Daten mit keinem oder einem geringen Schutzbedarf ergriffen werden, kann dies bedeuten, dass die Mitarbeiter zu viel Zeit aufwenden müssen, wenn sie auf die Daten zugreifen möchten und diese nach der Verarbeitung wieder verschließen. Schlimmstenfalls führt dies dazu, dass die Mitarbeiter die Schutzmaßnahmen aufgrund des Missverhältnisses nicht mehr ernst nehmen. Andererseits werden gerade im Gesundheitswesen viele sensible Daten und

Informationen gelagert. Für eine Einschätzung der Schutzgrade empfiehlt sich eine Orientierung an den gesetzlichen Vorgaben des Bundesdatenschutzgesetzes und des Strafgesetzbuches nach den Kategorien:

- kein Schutzbedarf
- normaler Schutzbedarf
- erhöhter Schutzbedarf
- höchster Schutzbedarf

Für alle Daten mit einem Schutzbedarf sollte dokumentiert werden, wo diese aufbewahrt bzw. gespeichert werden. Im Schadensfall kann so nachvollzogen werden welche Daten wo gelagert werden und welche Daten von einem unberechtigten Zugriff betroffen sein könnten. So kann unmittelbar nach einem Einbruch festgestellt werden, welche Informationspflichten an die Betroffenen und die Aufsichtsbehörden entstehen. Die Zusammenstellung der Daten und die Einschätzung ihres Schutzbedarfes dürfte nicht zu schwierig sein. Jede Institution unterliegt ohnehin der Pflicht, ein Verfahrensverzeichnis zu führen (s. Kap. V.4). Dieses enthält eine Aufstellung der Verfahren, der darin enthaltenen Daten und deren Schutzbedarf. Auf Basis des Verfahrensverzeichnisses kann dann eine Aufstellung erfolgen, auf welchen Geräte Daten gespeichert sind und entsprechend nach dem Schutzbedarf kategorisiert werden. Diese Aufstellung wird ergänzt mit einer Dokumentation der notwendigen Schutzmaßnahmen, sodass ein Notfallplan entsteht.

Eine „Inventarisierung" der Daten könnte wie in Tabelle 6 dargestellt aussehen.

Tab. 6 „Inventarisierung" der Daten

Gerät, Informationen zu dem Gerät (Hersteller, Artikelnummer)	weitere Informationen	Daten/ Datenkategorien	Schutzbedarf der Daten	Schutzmaßnahmen
Kopierer Faxgerät	Leasinggerät (Vertragsnummer) Kontaktdaten (Leasinganbieter)	alle	alle	Regelmäßige Löschung des Speichers Authentifikationsverfahren Klärung mit Hersteller/Leasingpartner bzgl. Fernlöschung
Festrechner, Notebook, Tablet PC	Notfallnummer IT-Abteilung oder externer IT-Dienstleister	alle	alle	Verschluss in Schränken bei Arbeitsende, wenn möglich Abschließen der Räume Authentifikationsverfahren Verschlüsslung sensibler Daten Fernwartung/-löschung
Datenträger (USB-Sticks u.a.) Smartphones		alle	keine Daten mit erhöhten oder höchsten Schutzbedarf auf Datenträgern!	Verschluss in Schränken bei Arbeitsende Verschlüsslung

Gerät, Informationen zu dem Gerät (Hersteller, Artikelnummer)	weitere Informationen	Daten/ Datenkategorien	Schutzbedarf der Daten	Schutzmaßnahmen
Kartenlesegerät	Notfallnummer Bank, Krankenkassen	Bank-/ Zahlungsdaten, Daten der Gesundheitskarte	höchster Schutzbedarf	Verschluss in Schränken bei Arbeitsende Verschlüsslung
Medizingeräte	Leasinggerät (Vertragsnummer) Kontaktdaten (Leasinganbieter)	Gesundheitsdaten, ggf. mit Name, Vorname, Versicherungsnummer	höchster Schutzbedarf	regelmäßige Löschung des Speichers Authentifikationsverfahren Klärung mit Hersteller/Leasingpartner bzgl. Fernlöschung
Daten in Papierform		alle	alle	„Clean-Desk-Policy“ Verschluss in Schränken bei Arbeitsende

5.3 Notfallplan – was tun bei Einbruch?

Auch wenn konsequent Maßnahmen zum Schutz der Gebäude ergriffen wurden, kann nicht ausgeschlossen werden, dass es dennoch zu einem Einbruch kommt. Für solche Fälle sollte man einen Notfallplan bereithalten, der im Schadensfall Punkt für Punkt abgearbeitet werden kann. Ein solcher Notfallplan könnte wie folgt aussehen:

- Benachrichtigung der Polizei
- Schadensmeldung an die zuständige Versicherung
- Prüfung des Verlustes – Geräte/Datenträger
  - gestohlene Geräte
    - Server, Festrechner, Notebook
    - Tablet PCs, Smartphones
    - Kopierer, Faxgerät
    - Kartenlesegerät
    - Datenträger (USB-Sticks u.a.)
    - Medizingeräte
  - gestohlene Akten
    - Schreibtische
    - aufgebrochene Schränke
    - durchwühlte Schubladen
- Prüfung der Daten
  - Geräte/Akten
    - Welche Daten wurden auf den gestohlenen Geräten gespeichert?
    - Welche Daten enthielten die entwendeten Akten?
    - Welchen Schutzbedarf haben die Daten?
    - Weisen die Daten Besonderheiten auf in Bezug auf (§ 42a BDSG):
      - Gesundheitsdaten
      - Berufsgeheimnis
      - Strafbare Handlungen oder Verdacht darauf?
      - Bank- und Kreditkartenkonten

- Maßnahmen
  - Back-up: Prüfung des letzte Status, sodass festgehalten werden kann, welche Daten ggf. komplett verloren gehen
  - Fernwartung: Einleitung zur Fernlöschung von Daten auf entwendeten Datenträgern
  - Information: Im Falle eines Datenverlustes gemäß § 42a BDSG Information des Verlustes an die Betroffenen und die Aufsichtsbehörden
- Konsequenzen
  - Revision: Prüfung, welche Sicherheitslücken den Einbruch ermöglicht haben könnten
  - Einführung neuer Maßnahmen

Besonderheiten bei „digitalen" Einbrüchen

Einbrüche beschränken sich nicht nur auf Einbrüche in den Geschäftsräumen. Sie können auch digital ausgeführt werden bzw. ein Einbruch in den Geschäftsräumen kann einen digitalen Einbruch zur Folge haben. Wird ein solcher Angriff bemerkt, sollten die betroffenen Geräte sofort abgeschaltet werden und sowohl vom Strom- als auch vom Computernetzwerk getrennt werden. Eine Anzeige gegen Unbekannt bei der Polizei sollte auch hier umgehend erfolgen.

Aufgrund der Komplexität der IT-Landschaften sollte ein Praxisinhaber nicht selber versuchen, mögliche Spuren auf dem Rechner zu sichern, sondern sich an Experten wenden. Dies können die entsprechenden Ansprechpartner in der Abteilung Computerkriminalität der Landeskriminalämter sein oder auch private Unternehmen sein, die sich auf Computerforensik spezialisiert haben. Diese Experten können dann den Angriff analysieren, das Schadensszenario umreißen und umfangreiche Sicherheits- und Sicherungsmaßnahmen ergreifen. Das selbstständige Eingreifen führt in den meisten Fällen zum Verwischen von Spuren, die einen Rückschluss auf Täter bzw. betroffene Datenbestände zulassen würden.

Da bei einem Angriff schnell die vollständige IT-Infrastruktur betroffen sein kann, sollte ein Vorfall auf keinen Fall auf die leichte Schulter genommen werden. Insbesondere bei der heutigen, starken Durchdringung der Geschäftsprozesse, kann eine Attacke auf die Sicherheit eines Computers einen Stillstand der Institution gleich kommen. Auch für digitale Einbrüche muss daher ein Notfallplan bestehen. Hinweise, wie ein komplexes Notfallmanagement aufgebaut werden kann, gibt die Broschüre „BSI-Standard 100–4 Notfallmanagement" des Bundesamtes für Sicherheit in der Informationstechnik.

Information an die Betroffenen und die Aufsichtsbehörden

Zu Beginn wurde bereits die Verpflichtung, bei Verlust von besonderen Daten die Betroffenen wie die zuständige Aufsichtsbehörde zu informieren, beschrieben (§ 42a BDSG). Die Benachrichtigung an den Betroffenen sollte zwar unverzüglich erfolgen, kann jedoch verzögert werden, wenn es sinnvoller ist zuvor Sicherheitslücken zu schließen. Dies gilt auch, wenn Maßnahmen zur Strafverfolgung eingeleitet werden, welche nicht durch eine Information an die Betroffenen beeinträchtigt werden sollten. Gegenüber den Aufsichtsbehörden ist eine verzögerte Mitteilung des entstandenen Schadens nicht möglich. Die Aufsichtsbehörde wird dabei nicht nur über den

Schaden und das Ausmaß des Schadens informiert, sondern auch über die ergriffenen Maßnahmen (vgl. Gola u. Schomerus 2015, § 42a BDSG, Rn. 5 und 6).

Grundsätzlich sind die Betroffenen individuell zu informieren. Dies ist jedoch bei einer sehr großen Anzahl von Betroffenen (z.B. wenn bei einem Sicherheitsangriff auf eine Krankenkasse mehrere Millionen Versicherte betroffen sind) nicht realistisch. Hier besteht die Möglichkeit, die Betroffenen über Medien mit entsprechender Reichweite zu informieren, z.B. mit Anzeigen in bundesweit erscheinenden Tageszeitungen oder mit Meldungen in bekannten Onlinediensten. Das Gesetz selbst spricht hier von „mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme". Bei einer Arztpraxis oder einer Apotheke kann daher eine Veröffentlichung in lokalen Medien oder durch einen Aushang besser geeignet sein.

Literatur

ARD (2015) Sicherheitsrisiko Kopierer: Hochsensible Daten frei Haus. Sendung „Plusminus" vom 21.10.2015, 21:45 Uhr. URL: http://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/daten-kopierer-speichern-100.html (abgerufen am 06.01.16)

Bayerisches Landesamt für Datenschutzaufsicht (LDA) (2014) Checkliste: Datensicherheit. Technisch-organisatorische Maßnahmen nach § 9 BDSG und Anlage. URL: https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Checkliste_Datensicherheit.pdf (abgerufen am 06.01.16)

Bundesamt für Sicherheit in der Informationstechnik (2008) BSI-Standard 100–4 Notfallmanagement. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf;jsessionid=5289F9348C1965AF5D325CF00EB0E2F8.2_cid368?__blob=publicationFile&v=1 (abgerufen am 26.01.16)

Bundesamt für Sicherheit in der Informationstechnik (2015) IT-Grundschutzkataloge, Maßnahmenkatalog M1 Infrastruktur. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M1Infrastruktur/m1infrastruktur_node.html (abgerufen am 07.01.16)

Gesellschaft für Datenschutz und Datensicherheit e.V. (o.J.) Muster zur Auftragsdatenverarbeitung gemäß § 11 BDSG. URL: https://www.gdd.de/downloads/materialien/muster/Mustervereinbarung_a7_11_BDSG.doc/view (abgerufen am 06.01.16)

Gewerkschaft der Polizei (2015) Sicherheit in Arztpraxen. URL: http://www.polizei-dein-partner.de/nc/themen/einbruchschutz/einbruchschutz-gewerbe/detailansicht-einbruchschutz-gewerbe/artikel/sicherheit-in-arztpraxen.html?tx_ttnews[sViewPointer]=2 (abgerufen am 06.01.16)

Gola P, Schomerus R (2015) Bundesdatenschutzgesetz Kommentar. 12. Aufl. 2015. C.H. Beck München

Verwaltungsgericht Hannover (2013) Scannen von Personalausweisen verstößt gegen PAuswG. Urteil v. 28.11.2013, Az. 10 A 5342/11. URL: http://www.telemedicus.info/urteile/Datenschutzrecht/1499-VG-Hannover-Az-10-A-534211-Scannen-von-Personalausweisen-verstoesst-gegen-PAuswG.html (abgerufen am 06.01.16)