Datenbank-Programmierung

Kapitel 6: Datenschutz: Einführung

Prof. Dr. Stefan Brass

Martin-Luther-Universität Halle-Wittenberg

Sommersemester 2024

http://www.informatik.uni-halle.de/~brass/dbp24/

Lernziele

Nach diesem Kapitel sollten Sie Folgendes können:

- Einige Vorgehensweisen von Hackern erklären.
- Sicherheitsrelevante DBMS Funktionen erklären.
- Einige Grundzüge des deutschen Datenschutzrechtes beim Aufbau von Datenbanken berücksichtigen.

  Oder zumindest erkennen, wann Sie weitere Informationen einholen müssen.

Inhalt

DB-Sicherheit: Motivation (1)

- Information: wichtiger Aktivposten von Firmen.
  Darf nicht in die Hände der Konkurrenz gelangen.

  Z.B. Kundendaten, Einkaufspreise, Produkt-Zusammensetzungen.

- Es gibt Gesetze zum Schutz vertraulicher Daten.

  Wenn man z.B. zuläßt, dass ein Hacker Zugriff auf Kreditkartennummern bekommt und diese Daten dann mißbraucht, können hohe Schadenersatzforderungen entstehen. Außerdem: schlechte Reputation.

- Die Vertraulichkeit von Daten muss auch innerhalb der Firma geschützt werden (z.B. Gehälter).

  Man muss auch verhindern, dass Angestellte einfach alle Daten mitnehmen können, wenn sie die Firma verlassen.

DB-Sicherheit: Motivation (2)

- Falls es einem Hacker gelingen sollte, alle Daten zu löschen, oder vollständig durcheinander zu bringen, entsteht ein gewaltiger Schaden für die Firma.

  Darunter fällt auch die Erpressung durch Verschlüsselungstrojaner. Man sollte mindestens noch Sicherungskopien haben, auch offline, und an einem anderen Ort untergebracht (wegen einem möglichen Brand im Rechnerraum). Aber die Wiederherstellung dauert, und die letzten Änderungen sind schwer zu rekonstruieren.

- Unautorisierte Änderungen / Verfälschungen der Daten müssen verhindert werden, z.B. sollten Angestellte nicht ihr eigenes Gehalt ändern können.

  Bestimmte Geschäftsregeln — wer darf was tun — sollten durch das Informationssystem automatisch sichergestellt werden.

Sicherheits-Anforderungen (1)

Es sollte möglich sein ...

- sicher zu stellen, dass nur die tatsächlich legitimierten Benutzer Zugriff auf die Datenbank haben.

  $\rightarrow$ *Benutzer Identifikation/Authentifikation*

- festzulegen, welcher Nutzer welche Operationen auf welchen DB-Objekten durchführen darf.

  $\rightarrow$ *Benutzer-Autorisierung*

- die Aktionen der Benutzer zu protokollieren.

  $\rightarrow$ *Auditing*

Sicherheits-Anforderungen (2)

Es sollte auch möglich sein ...

- die Benutzung von Resourcen (Platten-Platz, CPU-Zeit) für jeden Nutzer zu begrenzen (Quotas).

  Sonst kann ein einzelner Nutzer die ganze Datenbank zum Stillstand bringen.

- Gruppen von Benutzern mit den gleichen Rechten zu verwalten.

  Umgekehrt kann ein Nutzer auch unterschiedliche Rollen haben.

- mehrere Administratoren mit unterschiedlichen Befugnissen zu haben.

  Nicht nur einen einzelnen Nutzer „root“, der alles darf.

Sicherheits-Anforderungen (3)

Es sollte auch möglich sein ...

- die Vertraulichkeit und Integrität der Daten auch in einer Netzwerk-Umgebung zu garantieren.

  Früher geschah die Client-Server Kommunikation oft unverschlüsselt.

- sicher zu stellen, dass niemand direkten Zugriff auf die Daten hat (und damit die Zugriffskontrolle der Datenbank umgeht).

- darauf zu vertrauen, dass nicht durch Programmierfehler im DBMS Sicherheitslücken bestehen (oder sie wenigstens schnell korrigiert werden).

Benutzer-Authentifikation (1)

- Üblich ist, dass sich Benutzer mit Passworten gegenüber dem System ausweisen.
- Zum Teil führen die DBMS selbst eine Benutzer-Identifikation durch, zum Teil verlassen sie sich auf das Betriebssystem.

  Beide Möglichkeiten haben Vor- und Nachteile: Es ist bequem, nicht mehrfach Passworte eingeben zu müssen, und es ist besser, wenn Anwendungsprogramme keine Passworte enthalten. Aber in einer Client-Server-Umgebung kann man nicht so sicher sein, dass der Benutzer auf dem Client tatsächlich die Person ist, die er/sie behauptet, zu sein (und dass der Computer wirklich der richtige Computer ist). Manche Client-Betriebssysteme haben ein schwächeres Sicherheitssystem als der Server (bei manchen PCs kann jeder eine Boot-CD einlegen).

Benutzer-Authentifikation (2)

- Es ist gefährlich, wenn des gleiche Passwort immer wieder genutzt wird.

  Wenn ein Hacker das Passwort irgendwie beobachten kann, kann er es auch nutzen. Z.B. kann man Listen mit Einmal-Passworten (TANs) verwenden.

- Einige Administratoren zwingen die Nutzer, ihre Passworte in regelmäßigen Abständen zu ändern.

  Z.B. jeden Monat. Dies kann aber zu schwächeren Passworten führen, (und zu häufigeren Problemen mit vergessenen Passworten), als wenn der Benutzer ein neues Passwort nur wählt, wenn er dazu bereit ist. Wenn ein System den Benutzer zwingt, sein Passwort zu ändern, prüft es üblicherweise auch, dass neues und altes Passwort sich deutlich unterscheiden, und dass der Benutzer nicht zu schnell zurück wechselt.

Benutzer-Authentifikation (3)

- Trojaner sind Programme, die neben der Hauptfunktion, für die sie eingesetzt werden, im Verborgenen noch andere (schlechte) Dinge tun.
- Speichern Sie keine wichtigen Passworte für andere Computer/Dienste auf der Festplatte Ihres Computers. Das gilt auch für Cookies, die Passworte ersetzen.

  Wenn Sie sich auf diese Art bei dem anderen Rechner einloggen können, ohne ein Passwort einzugeben, kann das auch jemand, der sich (z.B. mit Trojaner) die entsprechenden Daten von Ihrem System besorgt. Wenn das Passwort in einer Datei steht, ist es besonders einfach, und betrifft auch Passworte, die Sie nicht nutzen, wenn der Trojaner aktiv ist. Je nach Betriebssystem könnte er aber auch Tastendrücke mitloggen oder den Hauptspeicher anschauen.

Benutzer-Authentifikation (4)

- Passworte sollten nicht leicht zu raten sein.

  Der Name Ihrer Freundin/Ihres Freundes, Ihrer Lieblings-Popgruppe (Autor, Schauspieler, Film, Urlaubsland, etc.), Ihre Telefonnummer, Adresse, Geburtsdatum wären besonders leicht. Falls es einem Hacker gelingt, an eine verschlüsselte Version Ihres Passwortes zu kommen, kann er mit einer schnellen Verschlüsselungsroutine viele Worte probieren (selbst wenn eine direkte Entschlüsselung nicht möglich ist). Ein Hacker würde in so einem Fall den Duden durchprobieren, alle Namen von Personen, Popgruppen, relativ lange Folgen von Ziffern, zumindest alle kurzen Folgen von Kleinbuchstaben, etc. Außerdem alles auch rückwärts und auf verschiedene andere Arten leicht verändert. Deswegen wird empfohlen, dass ein gutes Passwort nicht zu kurz sein sollte, und Buchstaben, Ziffern, und Sonderzeichen enthalten sollte. Um eine möglichst zufällige Buchstabenfolge zu bekommen, kann man sich einen Satz denken und davon die Anfangsbuchstaben nehmen.

Benutzer-Authentifikation (5)

- Wenn ein System mehrere Anmeldeversuche mit falschem Passwort entdeckt, sollte es einen Alarm auslösen und eventuell den Account sperren.

  Außerdem gibt es oft eine künstliche Verzögerung, bevor das Programm dem Benutzer mitteilt, dass die Anmeldedaten falsch waren. So kann ein Hackerprogramm nicht viele Worte in kurzer Zeit probieren. Das Sperren des Accounts bestraft aber den korrekten Nutzer.

- Viele DBMS haben Default-Passworte für den Administrator. Diese müssen sofort geändert werden.

  Z.B. hat in Oracle der automatisch angelegte Administrator-Account `SYSTEM` das Passwort `MANAGER`, und das Passwort für `SYS` (kann alles) ist `CHANGE_ON_INSTALL`. Jeder Hacker weiß das. In SQL Server hat der mächtigste Account `sa` direkt nach der Installation kein Passwort.

Benutzer-Authentifikation (6)

- Man sollte Gast-Accounts löschen oder sperren.

  Oracle hat/hatte einen Account `SCOTT` mit Passwort `TIGER`. SQL Server hat einen Account `guest`, für Windows-Nutzer, die der Datenbank unbekannt sind. Prüfen Sie die Accounts im System in regelmäßigen Abständen und sperren Sie alle, die nicht wirklich benötigt werden.

- Das die meisten DBMS Client-Server Systeme sind, ist der DB-Server automatisch am Netz, sobald Ihr Rechner mit dem Internet verbunden ist.

  In dieser Hinsicht verhält sich der DB-Server ähnlich wie ein Web-Server. Selbst wenn der Hacker sich nicht beim Betriebssystem anmelden kann, kann er sich vielleicht bei der Datenbank anmelden.

Benutzer-Authentifikation (7)

- Wird ein Passwort unverschlüsselt über das Internet verschickt, können es Hacker eventuell lesen.
  - Beim klassischen Ethernet kann man alle Pakete mitlesen, die über das Netz geschickt werden.

    Mit modernen Switches ist das nicht mehr möglich, aber erst, nachdem der Switch die Adressen der angeschlossenen Rechner gelernt hat. Man kann sich also nicht darauf verlassen, dass andere Rechner, die an das lokale Netz angeschlossen sind, die Datenpakete nicht auch erhalten.
  - Die Route, die Datenpakete über das globale Internet nehmen, ist kaum vorhersehbar.

    Ein Gateway wird vielleicht von einem Hacker betrieben, oder ist schon von einem Hacker „geknackt“.

Benutzer-Authentifikation (8)

- Wenn Sie ein Passwort eingeben, achten Sie darauf, dass Sie auch mit dem richtigen Programm bzw. dem richtigen Computer verbunden sind.

  Früher gab es Programme, die wie ein UNIX Login Prompt aussahen, aber das Passwort an einen Hacker schickten.
  Der Suchpfad für Kommandos darf nur vertrauenswürdige Verzeichnisse enthalten (z.B. nicht „.“). Sonst bekommt man vielleicht ein ganz anderes Programm, wenn man z.B. „sqlplus“ aufruft.
  Es gibt viele „Phishing“ („password fishing“) EMails, die z.B. behaupten, von der eigenen Bank zu kommen, und zur Eingabe von PIN und TAN auffordern. Tatsächlich kommt man mit der URL aber auf eine Hacker-Webseite, die wie die echte Webseite der Bank aussieht.

Benutzer-Authentifikation (9)

- Man sollte möglichst nicht das gleiche Passwort für verschiedene Systeme (auch Webshops) nutzen.

  Angestellte des Webshops können Ihr Passwort möglicherweise im Klartext lesen. Es ist zwar üblich, Passworte nur verschlüsselt (z.B. MD5-Hash) zu speichern, aber es gibt keine Garantie, dass jeder Shop-Betreiber das auch so macht. Als Schutz gegen vorberechnete Listen von Hashes von Wörterbüchern („Rainbow Table“) wird dem Passwort eine längere, zufällige Zeichenkette angehängt („Salt“), die zusammen mit dem Hashwert in der Datenbank gespeichert wird.

- Sagen Sie Ihr Passwort (auch PIN etc.) nie offiziell klingenden Unbekannten am Telefon!

  Z.B. dem technischen Support des Rechenzentrums, das gerade auf LDAP umstellt, und Ihnen die Mühe ersparen möchte, ins Rechenzentrum zu kommen, und dort Ihr Passwort noch einmal einzutippen.

Sicherheitsmodelle

- Die Festlegung der Autorisierung („wer darf was mit welchen Daten tun?“) ist Gegenstand des nächsten Kapitels („Zugriffsrechte in SQL“).
- Es gibt zwei grundlegend verschiedene Sicherheitsmodelle. Normale Datenbanksysteme implementieren nur das erste:
  - „Discretionary Access Control“ erlaubt den Administratoren, die Zugriffsrechte nach Belieben zu vergeben.
  - „Mandatory Access Control“ basiert auf einer Klassifizierung von Benutzern und Daten.

    Z.B. „confidential“, „secret“, „top secret“. Benutzer können nur Daten auf der eigenen oder einer niedrigeren Sicherheitsebene lesen, und nur Daten auf der eigenen oder einer höheren Sicherheitsebene schreiben.

Auditing

- In manchen Systemen kann man die Aktionen der Benutzer mitprotokollieren lassen.

  Das könnte Ärger mit dem Betriebsrat geben, eventuell auch mit dem Datenschutz. Man beachte, dass nicht nur erfolgreich ausgeführte Kommandos protokolliert werden müssen, sondern auch Kommandos, die z.B. wegen nicht ausreichender Zugriffsrechte abgelehnt wurden.

- So kann man wenigstens hinterher herausfinden, wer für ein Problem verantwortlich ist.

- Eventuell fallen bei einer Kontrolle auch merkwürdige Muster auf, bevor wirklich ein Schaden eintritt.

  Man muss sehr selektiv mitprotokollieren, wenn man im Protokoll wirklich noch etwas Interessantes finden will.

Datensicherheit

- Niemand (der nicht ohnehin DBA Rechte hat) sollte direkten Zugriff auf die Daten haben (und damit die Zugriffskontrolle der Datenbank umgehen).

  Aus Performance-Gründen werden die Daten normalerweise unverschlüsselt in Betriebssystem-Dateien gespeichert. Wer auf diese Dateien Zugriff hat, kann auch ohne DB-Account die Daten darin lesen.

- Backup Bänder müssen weggeschlossen werden.

- In Deutschland wurde ein PC gestohlen, der ein AIDS-Register enthielt. In den USA sind mehrere Notebooks der CIA mit geheimen Unterlagen verschwunden.

Inhalt

Datenschutz-Recht (1)

- In diesem Abschnitt sollen einige Vorschriften der europäischen Datenschutz-Grundverordnung (DSGVO oder DS-GVO) auszugsweise erklärt werden.

  Ich bin kein Jurist, und der zur Verfügung stehende Platz ist nicht ausreichend für eine vollständige Erklärung. Alle Angaben sind ohne Gewähr. Wenn es wirklich wichtig ist, informieren Sie sich bitte bei einem Juristen.

- Die DSGVO ist seit dem 25. Mai 2018 gültig.

- Eine EU-Verordnung gilt unmittelbar in jedem Mitgliedsland.

  Dagegen sind „Richtlinien“ nur Zielvorgaben, die in nationales Recht umgesetzt werden müssen (innerhalb einer vorgegebenen Frist). Vor der DSGVO gab es die Richtlinie 95/46/EG und das „alte Bundesdatenschutzgesetz“.

- Englisch: General Data Protection Regulation (GDPR).

Datenschutz-Recht (2)

- Der Text der DSGVO ist z.B. hier verfügbar:
  - [https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679]

    Das dort auch erhältliche PDF hat 88 Seiten, von denen die ersten 31 Seiten „Erwägungsgründe“ sind, also eine Art Kommentar.
  - [https://.../?uri=CELEX:02016R0679-20160504]

    Diese Version enthält Berichtigungen/Aktualisierungen bis 2021.
  - [https://dsgvo-gesetz.de/]
  - [https://dejure.org/gesetze/DSGVO]
- Das Bundesdatenschutzgesetz (BDSG) ergänzt die DSVGO:
  - [https://www.gesetze-im-internet.de/bdsg_2018/]
  - [https://dsgvo-gesetz.de/bdsg/]

Datenschutz-Recht (3)

- Datenschutzgesetze sollen davor schützen, dass man durch Umgang mit seinen personenbezogenen Daten in seinem verfassungsmäßig garantierten Persönlichkeitsrecht beeinträchtigt wird (freie Selbstbestimmung bei der Entfaltung der Persönlichkeit).
- Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 war wegweisend und enthält u.a. folgende Begründung:

  „Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“

Datenschutz-Recht (4)

- Es soll vermieden werden, dass „Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß.“
- Man soll normalerweise selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen können („Informationelle Selbstbestimmung“).
- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

  Siehe Art. 4 Nr. 1 DSGVO. Natürliche Person im Gegensatz zu juristischer Person (z.B. GmbH).

- Auch IP-Adressen gelten als personenbezogen.

  Gerichtsurteile: C-582/14 des EuGH (2016), VI ZR 135/13 des BGH (2017).
  Siehe: Dr. DSGVO. Kritischer: datenschutzticker.de

Rechtmäßigkeit der Datenverarbeitung (1)

- Verarbeitung personenbezogener Daten ist verboten, wenn nicht einer der folgenden Gründe vorliegt (Art. 6 DSGVO):
  - Einwilligung der betroffenen Person
  - Notwendig zur Erfüllung eines Vertrages mit der betroffenen Person (auch vorvertragliche Maßnahmen, z.B. Angebot).
  - Es gibt rechtliche Verpflichtung (z.B. Rechnung 10 Jahre).
  - Um lebenswichtige Interessen zu schützen (Notaufnahme).
  - Aufgabe im öffentlichen Interesse (z.B. „Knöllchen“).
  - Wahrung berechtigter Interessen des Verantwortlichen (d.h. der Firma) oder eines Dritten, sofern nicht Interessen bzw. Grundrechte der betroffenen Person überwiegen.

Rechtmäßigkeit der Datenverarbeitung (2)

Einwilligung:

- Die Einwilligung muss freiwillig erfolgen.

  Die Erfüllung eines Vertrags/Erbringung einer Dienstleistung darf nicht von der Einwilligung zur Verarbeitung personenbezogener Daten abhängig gemacht werden, die für diesen Zweck nicht erforderlich sind (Art. 7 (4) DSGVO) („Kopplungsverbot“). Es muss Alternativen geben, ggf. kostenpflichtige. Daten-gegen-Leistung muss transparent sein und dann ist ein Vertrag Rechtsgrundlage, nicht die freiwillige Einwilligung (LDI NRW 26. Bericht 2021).

- Einwilligungen können jederzeit widerrufen werden.

  Vorher erfolgte Verarbeitungen bleiben natürlich rechtmäßig. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

- Einwilligungen können nicht versteckt sein in Erklärungen, die noch andere Sachverhalte betreffen (klar unterscheidbar).

Rechtmäßigkeit der Datenverarbeitung (3)

Berechtigtes Interesse/Werbung:

- Das Versenden von Werbung per Post ist von den „berechtigten Interessen“ gedeckt, Werbung per EMail bedarf dagegen nach dem § 7 UWG (Gesetz gegen unlauteren Wettbewerb) einer Einwilligung.

  Siehe: Michael Rohrlich: Datenschutz einfach umsetzen, S. 38, 40.
  Es gibt allerdings das „Bestandskundenprivileg“: Falls der Unternehmer die Email-Adresse vom Kunden erhalten hat, und es um eigene ähnliche Waren geht, der Kunde nicht widersprochen hat, und der Kunde bei Erhebung sowie jeder Verwendung auf die Widerspruchsmöglichkeit hingewiesen wird, stellt die EMail keine unzumutbare Belästigung dar (ist also legal).

- Gegen Verarbeitung aufgrund von „berechtigtem Interesse“ besteht in bestimmten Situationen ein Widerspruchsrecht (Art. 21 DSGVO), insbesondere auch bei Direktwerbung.

Rechtmäßigkeit der Datenverarbeitung (4)

Besonders schützenswerte, sensitive Daten:

- „Besondere Kategorien personenbezogener Daten“ sind (Art. 9 DSGVO):
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Genetische und biometrische Daten
  - Gesundheit
  - Sexualleben, sexuelle Orientierung
- Für diese Daten gelten verschärfte Vorschriften.

  Insbesondere entfällt die Rechtfertigung „berechtigtes Interesse“.

Rechtmäßigkeit der Datenverarbeitung (5)

Zweckbindung:

- Daten müssen „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“ (Art. 5 DSGVO).

  Im öffentlichen Interesse liegende Archivzwecke, sowie wissenschaftliche, historische und statistische Zwecke sind ausgenommen.

- Es gibt allerdings eine etwas verschwommene Klausel in Art. 6 (4) DSGVO. Demnach kann die Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar sein. Siehe auch Informationspflicht nach Art. 13 (3) DSGVO.

  [https://www.dr-datenschutz.de/dsgvo-zweckaenderung-der-datenverarbeitung-am-beispiel-werbung/]

Rechtmäßigkeit der Datenverarbeitung (6)

Speicherfrist:

- Personbezogene Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“ (Art. 5 DSGVO).
- In anonymisierter Form dürfen sie natürlich beliebig lange gespeichert werden.

  Dann sind es ja auch keine personenbezogenen Daten mehr.
- Es müssen natürlich weitere Rechtsvorschriften beachtet werden, z.B. sind Rechnungen 10 Jahre aufzubewahren.

  Siehe § 257 HGB und § 14b UStG.
- Siehe auch Art. 17 DSGVO für die Pflicht zur Löschung.

Rechtmäßigkeit der Datenverarbeitung (7)

Weiteres:

- Im BDSG ergänzen § 22–31 die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, insbesondere bezieht sich § 26 BDSG auf Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses.
- Falls eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen hat, ist vorab eine Datenschutz-Folgenabschätzung erforderlich.

  Siehe Art. 35 DSGVO. Es kann außerdem eine vorherige Konsultation der Aufsichtsbehörde nötig sein (Art. 36 DSGVO).
- Die DSGVO gilt nicht für ausschließlich persönliche oder familiäre Tätigkeiten (Art. 2 (2) DSGVO).

  Wenn man Fotos ins Internet stellt, ist es nicht mehr ausschließlich persönlich.

Datenschutzbeauftragte (1)

- Öffentliche Stellen, die personenbezogende Daten verarbeiten, müssen einen Datenschutzbeauftragten bestellen.
- Ebenso Firmen, deren Kerntätigkeit darin besteht, systematische Überwachung von Personen durchzuführen oder sensible Daten (Folie 29) in großem Umfang zu verarbeiten (Art. 37 DSGVO).
- Firmen, bei denen mindestens 20 Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt sind, brauchen auch einen Datenschutzbeauftragten (§ 38 BDSG).
- Der Datenschutzbeauftragte muss Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis haben.
- Er/Sie ist in Ausübung dieser Tätigkeit weisungsfrei.

Datenschutzbeauftragte (2)

- Es darf keinen Interessenskonflikt geben (Art. 38 DSGVO).

  Z.B. Geschäftsführer und IT-Abteilungsleiter kommen nicht in Frage.

- Der/Die Datenschutzbeauftragte muss der Aufsichtsbehörde gemeldet werden und Kontaktdaten müssen (z.B. auf der Webseite) veröffentlicht werden.

- Aufgaben des Datenschutzbeauftragten (Art. 39 DSGVO):
  - Beratung des Managements (des Verantwortlichen),
  - Schulung der Benutzer in den Datenschutz-Vorschriften,
  - Überwachung der Einhaltung der Rechtsvorschriften,
  - Zusammenarbeit mit der Aufsichtsbehörde,
  - Ansprechpartner für betroffene Personen (§ 6 (5) BDSG).

Informationspflicht (1)

- Wenn Daten bei der betroffenen Person erhoben werden, sind folgende Infornationen mitzuteilen (Art. 13 DSGVO):
  - Name und Kontaktdaten des Verantwortlichen,

    sowie ggf. des Datenschutzbeauftragten,
  - die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung,

    Im Falle von „berechtigten Interessen“ sind diese aufzulisten. Könnte die Person die Daten auch nicht bereitstellen, mit welchen Konsequenzen?
  - Informationen zur Weitergabe der Daten,
  - die Dauer der Speicherung (bzw. Kriterien dafür),
  - Aufklärung über Rechte des Betroffenen

    Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Datenübertragbarkeit, Widerrufen einer Einwilligung, Beschwerderecht bei Aufsichtsbehörde.

Informationspflicht (2)

- Für automatisierte Entscheidungsfindung gibt es zusätzliche Regeln (Art. 22 DSGVO), wozu auch die Offenlegung der Logik gehören kann (Art. 13 DSGVO).
- Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, ergibt Art. 14 DSGVO im Prinzip die gleichen Informationspflichten, jetzt aber mit mehr Ausnahme-Möglichkeiten.
- Man braucht sowohl für Online- wie für Offline-Verarbeitung personenbezogener Daten eine Datenschutzerklärung.

Beispiel: [https://www.ldi.nrw.de/datenschutz/medien-und-technik/websites-muster-fuer-datenschutzhinweise]

Verzeichnis von Verarbeitungstätigkeiten (1)

- Jeder Verantwortliche muss ein „Verzeichnis von Verarbeitungstätigkeiten“ führen und dieses auf Anfrage der Aufsichtsbehörde zur Verfügung stellen (Art. 30 DSGVO).
- Dies enthält Namen und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten und pro Tätigkeit:
  - Zweck der Verarbeitung,
  - Kategorien betroffener Personen,
  - Kategorien personenbezogener Daten,
  - Kategorien von Empfängern,

    Das können auch die eigenen Mitarbeiter sein, die zugriffsberechtigt sind.

    Besonders kritisch: Datenübermittlungen in ein Drittland.
  - Fristen für Löschung (soweit möglich).

Verzeichnis von Verarbeitungstätigkeiten (2)

- Außerdem müssen technische und organisatorische Maßnahmen (TOMs) für die Sicherheit der Daten dokumentiert werden (Art. 32 DSGVO).

  Man darf es Hackern nicht allzu leicht machen, sondern muss sich um Sicherheit auf dem aktuellen Stand der Technik kümmern.
  Negativ-Beispiel: Account eines Dienstleisters war 5 Jahre nach Vertragsende nicht gesperrt, Bankdaten inkl. Postident/Personalausweis-Kopie entwendet: Urteil LG München I, 09.12.2021 (2500 € Schmerzensgeld). Weiteres Urteil für anderen Kunden: LG Köln 28 O 328/21 (1200 €). 33.200 Kunden betroffen.

- Einfaches Beispiel eines Verzeichnisses von Verarbeitungstätigkeiten (Einzelhändler):
  [https://www.lda.bayern.de/media/muster/muster_12_einzelhaendler_verzeichnis.pdf]

  [https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf]

Rechte der betroffenen Personen (1)

Recht auf Auskunft:

- Nach Art. 15 DSGVO hat die betroffene Person das Recht, eine Bestätigung zu bekommen, ob sie betreffende personenbezogene Daten verarbeitet werden, und falls ja, folgende Informationen zu bekommen:
  - Verarbeitungszwecke,
  - Kategorien personenenbezogener Daten,
  - Empfänger gegenüber denen die Daten offengelegt wurden oder noch werden,
  - Speicherdauer,
  - falls die Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen zur Herkunft der Daten,

Rechte der betroffenen Personen (2)

Recht auf Auskunft, Forts.:

- Zu liefernde Informationen, Forts.:
  - Hinweis auf Rechte,
  - im Falle einer automatisierten Entscheidungsfindung Informationen zur Logik, Tragweite, angestrebten Auswirkungen,

    Dies bezieht sich nur auf automatisierte Entscheidungsfindung gemäß Art. 22 DSGVO (1) und (4), was ohnehin rechtlich kiritisch ist. Der Begriff „Profiling“ ist definiert in Art. 4 Nr. 4 DSGVO, und enthält z.B. die Bewertung/Analyse/Vorhersage der wirtschaftlichen Lage, von Vorlieben/Interessen oder des Aufenthaltsorts.
  - Im Falle der Übermittlung in ein Drittland die geeigneten Garantien für den Datenschutz und durchsetzbare Rechte (Art. 46 DSGVO).

Rechte der betroffenen Personen (3)

Recht auf Auskunft, Forts.:

- Dem Recht auf Auskunft muss normalerweise kostenlos entsprochen werden.

  Es kann nur abgelehnt werden, wenn es offensichtlich unbegründet ist oder rechtsmissbräuchlich erfolgt, also exzessiv häufig neu angefragt wird.
  In diesem Fall kann auch ein Entgelt verlangt werden (Art. 12 (5) DSGVO).

- Es ist wichtig, dass Auskünfte nur an die betroffene Person gegeben werden (erfordert Identitätsfeststellung).

  Z.B. schickt die Schufa die Datenkopie nach Art. 15 DS-GVO per Post an die Meldeadresse. Andere Unternehmen verlangen eine Personalausweis-Kopie (Teile dürfen darauf geschwärzt sein). Wenn die Person z.B. als Kunde ein Login in einem Webshop hat, sind die Daten des Benutzerkontos dort ohnehin einsehbar, und es könnte nach dem Login auch eine Zusammenstellung der Daten nach DSGVO angeboten werden.

Rechte der betroffenen Personen (4)

Recht auf Auskunft, Forts.:

- Der Bundesbeauftragte für Datenschutz und die Informationsfreiheit (BfDI) sagt, dass die Auskunft auch Kopien von Korrespondenz enthalten muss (also nicht nur Zeilen der DB).

  [https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html]

- Das Bundesdatenschutzgesetz (§ 34 BDSG) enthält einige Einschränkungen.

  Das Auskunftsrecht besteht nicht, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder nur Zwecken der Datensicherung und der Datenschutzkontrolle dienen, und die Auskunftserteilung unverhältnismäßigen Aufwand erfordern würde. Backup-Medien müssen also nicht durchsucht werden. Weitere Ausnahmen, wenn zivilrechtliche Ansprüche oder die öffentliche Sicherheit und Ordnung gefährdet sind.

Rechte der betroffenen Personen (5)

Musterschreiben Auskunftsrecht:

- (Quelle: Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg)

  In den Erläuterungen zum Schreiben wird auf die Identifizierbarkeit hingewiesen. Dazu sollen Sie neben der vollständigen Adresse z.B. Kunden- und/oder Rechnungsnummer angeben (eventuell auch das Geburtsdatum). Besonders bei einem Antwortwunsch per EMail ist die Identifizierung wichtig.

- Hiermit erbitte ich von Ihnen gemäß Art. 15 Abs. 1 DS-GVO unentgeltliche und schriftliche Auskunft, ob Sie mich betreffende personenbezogene Daten verarbeiten (Definition des Begriffs „Verarbeitung“ siehe Art. 4 Nr. 2 DS-GVO).

- Falls ja, schließe ich folgende Fragen an:

  - . . . (siehe folgende Folien)

Rechte der betroffenen Personen (6)

Musterschreiben Auskunftsrecht, Forts.:

- Fragen bei Verarbeitung von personenbezogenen Daten:
  - Welche mich betreffenden personenbezogenen Daten verarbeiten Sie?
  - Zu welchem Zweck (welchen Zwecken) verarbeiten Sie diese Daten?
  - Woher stammen diese mich betreffenden Daten?
  - Haben Sie diese Daten an Dritte übermittelt oder planen Sie, diese an Dritte zu übermitteln? Wenn ja, an wen, wann und zu welchem Zweck (welchen Zwecken)?
  - Wie lange werden Sie meine Daten verarbeiten (Stichwort Datenlöschkonzept)?

Rechte der betroffenen Personen (7)

Musterschreiben Auskunftsrecht, Forts.:

- Fragen, Forts.:
  - Haben Sie hinsichtlich meiner Person ein Profil angelegt? Falls ja, teilen Sie mir den Inhalt dieses Profils und die Art und Weise des Zustandekommens dieses Profils bitte mit.
  - Welchen aktuellen Scorewert übermitteln Sie hinsichtlich meiner Person und welche genaue Bedeutung hat dieser Scorewert? An wen haben Sie meinen Scorewert in den letzten 12 Monaten übermittelt? Welche einzelnen Daten liegen dieser Scorewertberechnung zugrunde?
    Woher haben Sie diese Daten?

    Diese Frage ist nur bei Wirtschaftsauskunfteien (Schufa etc.) zu stellen.

    Das unentgeltliche Auskunftsrecht besteht nur ein Mal pro Jahr.

Rechte der betroffenen Personen (8)

Musterschreiben Auskunftsrecht, Forts.:

- Fragen, Forts.:
  - Verarbeiten Sie die mich betreffenden Daten mithilfe einer weiteren automatisierten Entscheidungsfindung? Falls ja, erläutern Sie bitte mit aussagekräftigen Informationen die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen des bzw. der eingesetzten Verfahren.
- Ihre schriftliche Stellungnahme per Briefpost erwarte ich unverzüglich, spätestens aber innerhalb eines Monats (Art. 12 Abs. 3 DS-GVO) nach Eingang dieses Schreibens. Vielen Dank im Voraus.

Rechte der betroffenen Personen (9)

Recht auf Berichtigung:

- Nach Art. 16 DSGVO hat die betroffene Person das Recht, die Berichtigung sie betreffender falscher Daten zu verlangen.

  Dieses muss „unverzüglich“ geschehen. Auch die Vervollständigung unvollständiger Daten kann verlangt werden (machmal entsteht ein unrichtiger Eindruck gerade durch das Fehlen von Einträgen).

- Falls die Richtigkeit von personenbezogenen Daten bestritten wird, und die Überprüfung etwas länger dauert, kann in der Zwischenzeit auch die „Einschränkung der Verarbeitung“ nach Art. 18 DSGVO verlangt werden.

  Das bedeutet effektiv, dass die Daten als „gelöscht markiert“ werden, also nicht mehr in die normalen Verarbeitungsprozesse einbezogen werden. Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen und bei einem wichtigen öffentlichen Interesse dürfen sie allerdings verwendet werden.

Rechte der betroffenen Personen (10)

Recht auf Löschung / Recht auf „Vergessenwerden“:

- In den folgenden Fällen können die betroffenen Personen verlangen, dass Daten über sie gelöscht werden, und dies muss dann auch unverzüglich geschehen (Art. 17 DSGVO):
  - Die Daten sind für den ursprünglichen Zweck nicht mehr nötig.
  - Die betroffene Person widerruft ihre Einwilligung.

    Und es gibt keine andere Rechtsgrundlage für die Verarbeitung der Daten.
  - Wenn die Daten „aus berechtigtem Interesse“ gespeichert wurden, kann die betroffene Person ihr Widerspruchsrecht nach Art. 21 DSGVO ausüben.

    Dies geht immer für den Zweck der Direktwerbung, ansonsten muss die betroffene Person es mit ihrer besonderen Situation begründen, und es ist ggf. mit zwingenden schutzwürdigen Gründen abzuwägen.

Rechte der betroffenen Personen (11)

Recht auf Löschung, Forts.:

- Natürlich sind die Daten auch zu löschen, wenn sie unrechtmäßig verarbeitet wurden.
- Wenn „Angebote von Diensten der Informationsgesellschaft“ direkt einem Kind gemacht worden sind, so sind die dadurch erlangten Daten auf Wunsch zu löschen.
- Wenn der Verantwortliche die Daten öffentlich gemacht hat, und er zur Löschung verpflichtet ist, muss er angemessene Maßnahmen ergreifen, um Verantwortliche, die Kopien/Links verarbeiten, zu informieren, dass die Löschung verlangt wurde.

  Unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten.

Rechte der betroffenen Personen (12)

Recht auf Löschung vs. freie Meinungsäußerung:

- Es gibt offensichtlich einen Konflikt zwischen dem Recht auf Löschung und dem Recht auf freie Meinungsäußerung.
- Wenn sich Person A über Person B kritisch äußert (ggf. mit objektiv zutreffenden Fakten), sollte Person B nicht automatisch die Löschung erreichen können.

  Mindestens ein Politiker oder eine andere Person des öffentlichen Lebens sollten unliebsame Berichterstattung nicht einfach löschen lassen können.

- In Art. 17 (3) DSGVO ist eine Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information ausgenommen.

  Es bleibt aber formal ungeklärt, wo genau die Grenze liegt.

  Art. 85 DSGVO greift das noch einmal auf, aber erklärt nur, dass die Mitgliedsstaaten dafür selbst Regeln erlassen müssen.

Rechte der betroffenen Personen (13)

Weitere Ausnahmen vom Recht auf Löschung:

- Das Recht auf Löschung (Art. 17 DSGVO) gilt nicht, wenn die Verarbeitung erforderlich ist
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (z.B. Finanzamt),
  - für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (Art. 89 DSGVO),
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Nach § 35 BDSG teils nur „Einschränkung der Verarbeitung“.

Rechte der betroffenen Personen (14)

Musterschreiben mit Forderung der Löschung:

- Für Spammer gedacht ist das Musterschreiben „c't-Fassung von Framstags freundlichem Folterfragebogen“.
- Es enthält nach Beantragung der Auskunftserteilung noch folgenden Teil zur Löschung:
  - Weiterhin verlange ich nach Art. 17 DSGVO die unverzügliche Löschung meiner bei Ihnen verarbeiteten Daten.
  - Die Voraussetzungen des Art. 17 DSGVO liegen nach meiner Ansicht vor.
  - Sofern ich eine Einwilligung zur Verarbeitung meiner Daten erteilt habe, widerrufe ich diese hiermit, bzw. lege gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung ein. Dies gilt ebenso für das Profiling gemäß Art. 22 DSGVO.

Rechte der betroffenen Personen (15)

Musterschreiben mit Forderung der Löschung, Forts.:

- Forderungen, Forts.:
  - Lehnen Sie die Löschung ab, so haben Sie dies mir gegenüber zu begründen.
  - Sofern Sie meine personenbezogenen Daten öffentlich zugänglich gemacht haben und gemäß Art. 17 (1) DSGVO zu deren Löschung verpflichtet sind, haben Sie angemessene Maßnahmen zu ergreifen, um sämtliche Empfänger meiner Daten darüber gemäß Art. 19 DSGVO zu informieren, dass ich die Löschung aller Links zu diesen personenbezogenen Daten und von Kopien dieser personenbezogenen Daten verlangt habe.

Rechte der betroffenen Personen (16)

Weitere Rechte:

- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

  Falls die Verarbeitung auf Einwilligung oder auf einem Vertrag beruht, hat die betroffene Person das Recht, die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (soweit die Verarbeitung mithilfe automatisierter Verfahren erfolgt). Damit soll man den Anbieter wechseln können, ohne seine Daten zu verlieren. Allerdings dürfen damit die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden (manche Datensätze beziehen sich gleichzeitig auf zwei Personen).

- Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO).

Datenpannen (1)

- Eine Verletzung des Schutzes personenbezogener Daten („Datenpanne“, Art. 4 Nr. 12 DSGVO) liegt vor, wenn z.B.
  - eine Email mit personenbezogenen Daten an den falschen Empfänger geschickt wurde,

    Es ist auch nicht ok, eine Rundmail an eine große Zahl von Empfängern so zu verschicken, dass sie alle anderen Adressen sehen können ($\rightarrow$ `bcc`).
  - ein Hacker Zugriff auf den Rechner bekommt,

    Und Dateien mit personenbezogenen Daten kopiert.
  - ein USB-Stick mit personenbezogenen Daten verloren geht,

    Und die Daten nicht verschlüsselt waren.
  - ein Notebook/Smartphone mit solchen Daten gestohlen wird,

    Z.B. auch, wenn gebrauchte Notebooks verkauft werden, und eigentlich gelöschte Dateien darauf noch wiederhergestellt werden können.
  - Daten gelöscht wurden, die noch wichtig sein könnten.

Datenpannen (2)

- Nach Art. 33 DSGVO muss eine Datenpanne unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde (Art. 55 DSGVO) gemeldet werden,

  Die 72 Stunden beginnen vom Zeitpunkt der Kenntnis (durch irgendeinen Mitarbeiter) und werden auch durch Wochenende/Feiertage nicht unterbrochen.

- es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

  Beispiel für geringes Risiko (Landesbeauftragter für Datenschutz Niedersachsen): Falsche Anlage zu Hotelrechnung: Nur Namen und gebuchte Daten, aber keine Adressen oder gar Bankverbindungen.

- Für Inhalte der Meldepflicht siehe Art. 33 (3) DSGVO.

  Sie enthält auch eine Beschreibung der wahrscheinlichen Folgen und Maßnahmen zur Behebung der Schutzverletzung und zur Abmilderung ihrer negativen Folgen.

Datenpannen (3)

- Bei „voraussichtlich hohem Risiko für die persönlichen Rechte und Freiheiten“ müssen nach Art. 34 DSGVO die betroffenen Personen unverzüglich informiert werden.

  Der Europäische Datenschutzausschuss (EDSA/ EDPB) hat in den Leitlinien 01/2021 Beispiele für die Meldung von Verletzungen des Schutzes personenbezogener Daten zusammengestellt.

  - Wenn z.B. Kreditkartendaten bekannt geworden sind, kann der Betroffene seine Kreditkarte sperren lassen.

- Natürlich kann der Betroffene die Firma dann auf Schadensersatz und Schmerzensgeld verklagen.

  Selbst wenn das Schmerzensgeld (ohne objektiv zu beziffernden Schaden) in Deutschland im einzelnen Fall nicht besonders hoch ist, kann es sich bei vielen Betroffenen natürlich aufsummieren.

Literatur/Quellen

- Michael Rohrlich: Datenschutz einfach umsetzen.
  Akademische Arbeitsgemeinschaft, 2023, ISBN 978-3-96533-286-7, 264 Seiten.
- Bayrisches Landesamt für Datenschutzaufsicht (Hrsg.):
  Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine.
  C.H.Beck, 2017, ISBN 978-3-406-71662-1, 64 Seiten.
- Ralph Wagner: Vorlesung Datenschutztecht. TU Dresden, Sommersemester 2018.
  [https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_datenschutzrecht/1-Teil-Vorlesung-DS-Recht.pdf]
- Dresdner Institut für Datenschutz: Arbeitshilfen. [https://www.dids.de/arbeitshilfen/]
- Ruth Janal: Vorlesung Technikrecht — Datenschutz: Einführung.
  [https://www.zivilrecht8.uni-bayreuth.de/pool/dokumente/PDFs/6-Datenschutz.pdf]
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein:
  Tätigkeitsbericht 2023. [https://www.datenschutzzentrum.de/tb/tb41/]
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI):
  Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterungen.
  [https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.html]
- Datenschutzkonferenz. [https://www.datenschutzkonferenz-online.de/]
- EDSA: Datenschutzleitfaden für kleine Unternehmen.
  [https://www.edpb.europa.eu/sme-data-protection-guide/home_de]