DSGVO für Datenbankentwickler

Version 1.0.2 vom 27.1.2020

Inhalt und Ziele

Dieses Whitepaper bietet IT-Fachleuten und speziell Datenbankentwicklern die für sie wesentlichen Informationen und Handlungsanleitungen zur DSGVO in konzentrierter Form und verständlicher Sprache. Aus dem Wust an Gesetzestexten, Büchern, Webseiten und Artikeln zur DSGVO, zu Datenschutz und Datensicherheit filtern wir das, was der Praktiker tatsächlich wissen, verstehen und umsetzen muss.

Die technische Umsetzung anhand von Microsoft Access und Microsoft SQL Server behandeln wir in eigenen Abschnitten. Die weiteren Inhalte beziehen sich nicht auf bestimmte Datenbanksysteme, denn die Anforderungen sind für alle gleich.

Unser Zugang zum Datenschutz ist die eigene berufliche Praxis als selbständige Entwickler und IT-Fachleute. Neben Erkenntnissen aus Seminaren, Vorträgen und Diskussionen fließen auch Erfahrungen aus unserer beratenden Tätigkeit und praktischen Umsetzung bei Kunden ein.

Wir sind keine Juristen. Dieses Whitepaper stellt unsere Einschätzung und Meinung zum Thema dar und ist keine Rechtsberatung.

Autoren

Karl Donaubauer, Wien

Web: donkarl.com, Kontakt: office@donkarl.com
Datenbankentwickler, MVP für Microsoft Access
Zertifizierter Datenschutzbeauftragter

Vorträge zur DSGVO in at, de und den USA. Beratung und praktische Umsetzung der DSGVO-Anforderungen bei Kunden und Entwickler-Kollegen in .at und .de.

Meine Haltung zur DSGVO:
Pragmatisch und positiv. Bewusster, proaktiver Umgang mit dem Thema und Verständlichkeit sind näher am Geist der Verordnung als der pseudojuristische Ansatz, sich mit vielen (oft unpassend und gedankenlos kopierten) Texten und Formalismen gegen alles und jeden absichern zu wollen.

Bernd Jungbluth, Horn

Web: www.berndjungbluth.de, Kontakt: info@berndjungbluth.de
Berater, Trainer und Datenbankentwickler zu mit und in Access und SQL Server
Zertifizierter Datenschutzbeauftragter (TÜV), Betriebswirt WA Dipl. Inh.

Vorträge und Seminare zu Datenschutz und Datensicherheit mit Access und SQL Server
Beide Themen spielen in meinen Beratungen, Trainings und Datenbankentwicklungen eine zentrale Rolle.

Meine Haltung zum Datenschutz
Datenschutz sehe ich als elementaren Bestandteil der Datenverarbeitung. Mein besonderes Interesse gilt dem technischen Aspekt – und das über die Verarbeitung personenbezogener Daten hinaus. Ausgehend vom Datenschutz konzentriere ich mich auf die Datensicherheit und IT-Sicherheit in Unternehmen.

Philipp Stiefel, Hofheim am Taunus

Web: https://codekabinett.com, Kontakt: phil@codekabinett.com
Softwareentwickler und Prozessberater

Kontakt zur DSGVO:
Softwareentwicklung und Beratung zu Anwendungs- und Datensicherheit im Widerstreit zwischen staatlicher Aufsicht und Regulierung (Finanzdienstleistungen) und dem Schutz personenbezogener Daten.

Meine Haltung zum Datenschutz:
Die DSGVO hat dem Umgang mit den Daten sowohl bei betroffenen Personen als auch den verantwortlichen Unternehmen endlich angemessene Aufmerksamkeit verschafft. Blinder, formaljuristischer Aktionismus ohne differenzierte Auseinandersetzung mit dem Thema sind kontraproduktive Auswüchse.

Inhaltsverzeichnis

Rollen und Begriffe

Die DSGVO verwendet einige definierte und etablierte Begriffe. In diesem Abschnitt erklären wir die Begriffe, die für das Verständnis des weiteren Textes unerlässlich sind.

Personenbezogene Daten

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“
- Definition gemäß Artikel 4.1. DSGVO

Besondere Kategorien

Einige dieser Informationen sind besonders schützenswert. In Artikel 9 der DSGVO werden diese als „Daten besonderer Kategorien“ bezeichnet und umfassen Daten zur rassischen und ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Betroffene Person

Jeder Mensch, dessen personenbezogene Daten gespeichert und verarbeitet werden, ist lt. DSGVO eine betroffene Person. Dazu gehören u.a. die eigenen Mitarbeiter und die Ansprechpartner bei Kunden, Lieferanten und Geschäftspartnern.

Verarbeitung von Daten

“jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;”
- Definition gemäß Artikel 4.2. DSGVO

Oder aus Sicht des Datenbankentwicklers: Alles, was man mit Daten anstellen kann.

Verantwortlicher

Die zentrale Rolle im Datenschutz ist der Verantwortliche. Er ist die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche hat umfangreiche Aufgaben und Pflichten, die wir in diesem Dokument erläutern.

Auftragsverarbeiter

Der Auftragsverarbeiter ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dabei hat er ähnliche Aufgaben und Pflichten zu erfüllen.

Datenschutzbeauftragter

Die Aufgaben des Datenschutzbeauftragten sind die konzeptionelle Beratung des Verantwortlichen und Schulung der Mitarbeiter. Er erstellt i.d.R. das Datenschutzkonzept und überwacht dessen Einhaltung, ist aber nicht persönlich für die Umsetzung und Ausführung zuständig. Zudem ist er der Ansprechpartner für Betroffene und die Aufsichtsbehörde.

Der Datenschutzbeauftragte kann ein interner Mitarbeiter oder ein externer Dienstleister sein.

Die Voraussetzungen für die Benennung eines Datenschutzbeauftragten beschreiben wir im Abschnitt "Datenschutzbeauftragter“.

Technische und organisatorische Maßnahmen

Alle Aktivitäten und Vorkehrungen, die eine sichere Verarbeitung von personenbezogenen Daten sicherstellen, werden unter dem Begriff „technische und organisatorische Maßnahmen“ (TOMs) zusammengefasst. Wir beschreiben sie näher im gleichnamigen Abschnitt.

Grundsätze der Verarbeitung

Bei der Verarbeitung personenbezogener Daten sind die in Artikel 5 DSGVO definierten Grundsätze einzuhalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Diese Prinzipien sind elementar für die DSGVO-konforme Datenverarbeitung. Besonders hervorheben möchten wir hier die Rechtmäßigkeit und die Zweckbindung. Die anderen Grundsätze sind nicht weniger relevant und fließen an den passenden Stellen in den Text ein.

Rechtmäßigkeit

Die Verarbeitung ist nur rechtmäßig, wenn eine Einwilligung der betroffenen Person vorliegt, sie zur Vertragserfüllung oder zur Erfüllung vorvertraglicher Maßnahmen (Angebot, Auftragsbestätigung etc.) stattfindet, wenn eine rechtliche Verpflichtung besteht, zum Schutz lebenswichtiger Interessen oder zur Wahrnehmung von Aufgaben im öffentlichen Interesse.

Eine besondere Ausnahme ist die Wahrung berechtigter Interessen des Verantwortlichen. Dabei sind die Interessen des Verantwortlichen und die der betroffenen Person gegeneinander abzuwägen.

Zweckbindung

Die personenbezogenen Daten dürfen nur zu einem eindeutigen und festgelegten Zweck erhoben werden. Eine Weiterverarbeitung zu einem anderen Zweck ist nur zulässig, wenn dieser mit dem ursprünglichen Zweck vereinbar ist.

Gesamtbetriebliche Aufgaben

Die praktische Umsetzung erfolgt in mehreren Schritten. Es beginnt mit einer Bestandsaufnahme. Diese zeigt den Umfang der Aufgaben und Pflichten, woraus sich die technischen und organisatorischen Maßnahmen zur Umsetzung ergeben.

Bestandsaufnahme

Eine Bestandsaufnahme kann sehr unterschiedlich ausfallen. Hierbei spielt die eigene Position und Sichtweise eine entscheidende Rolle:

- Selbständiger Datenbankentwickler als Unternehmer
  Verantwortlicher für seine eigene IT und Datenbestände und somit für die Umsetzung der DSGVO in seinem Unternehmen
- Selbständiger Datenbankentwickler als Auftragnehmer
  mit Projekten wie Erstellen von Datenbankanwendungen und Pflichtenheften, Performance-Optimierung, Beratungen etc.
- Angestellter in der IT
  Administrator, Datenbankentwickler etc.
- Angestellter in der Rolle des Datenschutzkoordinators

Es lohnt sich bei der Bestandsaufnahme neben der eigenen auch die Perspektiven der anderen Rollen einzunehmen. Wichtig hierbei ist das Einbeziehen aller relevanten Personen – von der Geschäftsführung über die Abteilungsleiter bis zu einzelnen Mitarbeitern. Die Form ist völlig frei. Es kann ein Word-Dokument, eine Excel-Tabelle, oder eine eigene Access-Datenbank sein.

Wir können an dieser Stelle keine allgemeingültige Vorlage für eine Bestandsaufnahme liefern, bieten aber im Anhang eine Checkliste.

Aufgaben und Pflichten

Aus der DSGVO ergeben sich Pflichten mit primärer Wirkung nach außen. Da ihre Erfüllung oder Nicht-Erfüllung von außen einfach zu erkennen ist, sollten sie zuerst angegangen werden. Danach sind die Aufgaben zu erledigen, die sich überwiegend nach innen richten.

Wie bereits erwähnt, greifen in der Praxis viele Tätigkeiten ineinander. Eine scharfe Trennung ist nicht möglich. Es geht uns hier um die Tendenz von außen nach innen, der wir daher in der Auflistung und Beschreibung der Pflichten folgen.

Informationspflichten

Jede Person soll wissen, wer welche Daten über sie erhebt und verarbeitet. Das ist der Kernpunkt im wichtigsten Prinzip der DSGVO: faire und transparente Verarbeitung. Aus diesem Grund ist die betroffene Person bei der Erhebung ihrer Daten über folgende Punkte zu informieren:

- Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zweck der Datenerhebung
- Rechtsgrundlage
- Speicherdauer
- Betroffenenrechte
- ggf. Weitergabe der Daten an Dritte oder ins Nicht-EU-Ausland

Artikel 13 und 14 der DSGVO nennen ca. 1 Dutzend weitere Punkte, die in der Information enthalten sein müssen, z.B. der Hinweis auf das Widerspruchsrecht insbesondere bei Direktwerbung.

Umstritten ist die Art und Weise der Übermittlung der Information. Manche beschreiben die Verarbeitung der Daten in einem Dokument, dass der Person bei der Datenerhebung überreicht oder zugesandt wird, die meisten verlinken bzw. verweisen auf die Datenschutzerklärung ihrer Website oder informieren in einem kurzen Text als Fußnote in E-Mails und Briefen.

Datenschutzerklärung

Sie umfasst alle Punkte aus den Informationspflichten und gehört auf die Webseite. Dies gilt vor allem dann, wenn dort über Kontaktformulare personenbezogene Daten erhoben werden. Aber auch ohne diese offensichtliche Erhebung der Daten ist sie relevant, werden bei einem Aufruf der Website doch die IP-Adressen der Besucher gespeichert, ggf. per Tracking-Tools wie Google-Analytics das Surfverhalten auf der Website analysiert u.v.m.

Vorlagen für Datenschutzerklärungen gibt es viele - im Internet bei den Aufsichtsbehörden, bei den zuständigen Kammern und bei externen Beratern. Woher auch immer die Vorlage stammt, sie ist fast immer an die eigene Wirklichkeit anzupassen.

Beispiel:
Der für die Unternehmenswebseite zuständige Mitarbeiter hatte die Datenschutzerklärung von einer Wordpress-Vorlage kopiert. Unter anderem eine detaillierte Beschreibung des Umganges mit personenbezogenen Daten aus dem Kontaktformular und aus Blog-Kommentaren. Auf die Frage, wo sich das Kontaktformular und der Blog befänden, musste er passen. Beides gab es auf der Webseite nicht.

Eine solche Datenschutzerklärung signalisiert Benutzern der Webseite, dass der Datenschutz in diesem Unternehmen nur als lästige Pflicht angesehen wird.

Wir haben die Datenschutzerklärung geprüft und um alle gegenstandslosen Punkte bereinigt. Danach war sie übersichtlich, glaubwürdig und nur noch halb so lang.

Webseiten und DSGVO sind ein wichtiges und umfangreiches Thema und sollten in Bezug auf die DSGVO überprüft und angepasst werden. Es sind viele Punkte zu beachten, z.B. Newsletter, Kontaktformulare, eingebundene Inhalte wie der Google-Zeichensatz „Font Awesome“ und Social-Media-Plug-Ins.

Dieses Thema ist zu umfangreich, um es an dieser Stelle erschöpfend zu behandeln. Daher verweisen wir auf einen Artikel der IHK München: https://www.ihk-muenchen.de/dsgvo-datenschutz-webseite/

Meldepflichten von Datenschutzverletzungen

Der Umgang mit Datenschutzverletzungen ist in der DSGVO in Artikel 33 und 34 geregelt.

- Besteht ein Risiko für die betroffenen Personen, sind Datenschutzverletzungen bei der Aufsichtsbehörde zu melden.
- Die Meldung hat innerhalb von 72 Stunden zu erfolgen.
- Besteht für die Betroffenen einer Datenschutzpanne ein hohes Risiko, dann sind auch diese von der Panne und ihren potenziellen Folgen zu informieren.
- Diese Meldung hat unverzüglich zu erfolgen.

Die Organisationstrukturen und Szenarien von Unternehmen unterscheiden sich stark. Daher variieren der Informationsfluss und das Handlungskonzept bei Datenschutzverletzungen. Um bei einer

Datenpanne schnell und effektiv handeln zu können, ist ein im Voraus erstelltes Handlungskonzept für die eigene Situation erforderlich.

Grundvoraussetzung ist die Schulung der Mitarbeiter. Diese sollten Datenschutzverletzungen erkennen. Nicht erkannte Datenschutzpannen können weder gemeldet noch Gegenmaßnahmen ergriffen werden.

Rechte der Betroffenen

Die betroffenen Personen können gemäß DSGVO Art. 15 bis 22 umfangreiche Rechte einfordern. Auf diesen Fall sollte der Verantwortliche vorbereitet sein, ist das Erfüllen der einzelnen Rechte doch mit einem nicht zu unterschätzenden Aufwand verbunden. Dieser lässt zwar sich mit organisatorischen Maßnahmen reduzieren, eine Standardempfehlung hierzu gibt es aufgrund der vielfältigen Szenarien jedoch nicht.

Hinweis:
Unabhängig von dem eingeforderten Recht ist immer die Identität des Anfragenden sicherzustellen. Hierzu ist ein angemessenes Verfahren der Identitätsprüfung zu etablieren. Werden die Daten einer falschen Person geliefert, gelöscht oder verändert, ist dies eine Datenschutzpanne.

- Recht auf Auskunft
  - Bestätigung über die Verarbeitung der Daten, inklusive Information zu Verarbeitungszweck, Kategorien der verarbeiteten Daten, Speicherdauer, Empfänger, Herkunft etc.
  - Kopie der personenbezogenen Daten
- Recht auf Berichtigung und Vervollständigung
  - Falsche Informationen korrigieren
  - Für den Zweck der Verarbeitung unvollständige Daten ergänzen
- Recht auf Löschung
  - Grundsätzlich ist unverzüglich zu Löschen.
  - Unter Berücksichtigung von Ausnahmen wie gesetzliche Aufbewahrungspflichten, anhängige Rechtsstreitigkeiten, öffentliches Interesse etc.
- Recht auf Einschränkung der Verarbeitung
  - Daten gegen die weitere Verarbeitung sperren
  - Daten vor Löschung schützen - Einschränkung gilt nur vorübergehend bis zur Klärung offener Punkte wie strittige Richtigkeit der Daten, Klärung von Rechtsstreitigkeiten etc.
- Recht auf Datenübertragbarkeit
  - Datenübertragung an den Betroffenen oder direkt zu einem anderen Verantwortlichen
  - In gängigem maschinenlesbarem Format
- Widerspruchsrecht
  - Verarbeitung der Daten einstellen
  - Bei Direktwerbung immer und ohne besondere Gründe
  - Bei anderer Verarbeitung mit individuellen Gründen
- Recht auf Einzelfallprüfung bei automatisierten Entscheidungen
  - Entscheidung durch eine natürliche Person überprüfen und bewerten lassen
  - Gilt bei Verarbeitungen mit rechtlicher Wirkung, wie Profiling etc. und nur unter bestimmten Voraussetzungen

Erfüllt der Verantwortliche die Rechte einer betroffenen Person nicht, kann sie sich bei der Aufsichtsbehörde beschweren. Über dieses Beschwerderecht muss der Verantwortliche informieren.

Fristen (DSGVO Art. 12.3)
Bei Eingang eines Antrages ist unverzüglich zu reagieren. Die betroffene Person muss innerhalb eines Monats über die gespeicherten Daten bzw. die ergriffenen Maßnahmen (Löschung, Korrektur,

Einschränkung etc.) informiert werden. In besonders komplexen Fällen lässt sich diese Frist mit einer guten Begründung um weitere 2 Monate verlängern. Diese Verlängerung mitsamt ihren Gründen ist dem Antragsteller mitzuteilen.

Auftragsverarbeitungsvertrag

Der Auftragsverarbeiter ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dabei unterliegt er den Weisungen des Verantwortlichen und setzt das vereinbarte Vorgehen um.

Die Weisungen, wie auch die vereinbarten TOMs, sind in einem Auftragsverarbeitungsvertrag (AVV) schriftlich festzuhalten. Das geht auch in elektronischer Form. Dabei geht die Initiative vom Auftraggeber/Verantwortlichen aus.

Im Vertrag ist festzuhalten, dass der Auftragsverarbeiter dem Verantwortlichen die Einhaltung des Vertrages nachweisen und ihm Überprüfungen ermöglichen muss, nach Ende der Verarbeitungstätigkeit die Daten zurückzugeben oder zu löschen sind u.v.m. Die genauen Inhalte des Vertrages sind in Artikel 28 DSVGO geregelt. Vorlagen für Verträge findet man bei Aufsichtsbehörden, Kammern und Verbänden.

Nach der initialen Prüfung sollten die Verträge regelmäßig auf Ihre Aktualität und Korrektheit sowie die Umsetzung bzw. Einhaltung geprüft werden. Dies gilt für den Verantwortlichen ebenso wie für den Auftragsverarbeiter.

Nach unserer Erfahrung liegt häufig kein schriftlicher Vertrag vor, selbst wenn es sich um einen klaren Fall von Auftragsverarbeitung handelt. In diesem Punkt ist die DSGVO im Wirtschaftsleben noch nicht überall angekommen, und es besteht in vielen Fällen noch Klärungs- und Handlungsbedarf. Dabei ist der AVV hilfreich, um die Rollen und Pflichten bei der Handhabung von personenbezogenen Daten zu definieren.

In der Praxis ist nicht immer klar, ob man nun Auftragsverarbeiter ist oder eine andere Rolle innehat. Nehmen wir einen Softwareentwickler. Verwendet er nur Testdaten und hat keinen Zugriff auf die Echtdaten, gilt er nicht als Auftragsverarbeiter, und somit ist auch kein AVV notwendig. Wohingegen ein externer Netzwerkadministrator ein Auftragsverarbeiter sein kann. Er administriert die Produktivsysteme und hat dadurch Zugang zu Datenträgern und Dateien mit personenbezogenen Daten.

Nicht trivial ist auch die Abgrenzung zwischen Auftragsverarbeiter und eigenständigem Verantwortlichen. So gelten z.B. Steuerberater und Rechtsanwälte nicht als Auftragsverarbeiter, da sie in der Ausübung ihrer Aufgaben nicht weisungsgebunden sind.

Verarbeitungsverzeichnis

Das Verarbeitungsverzeichnis enthält alle Verarbeitungstätigkeiten mit personenbezogenen Daten in einem Unternehmen. Es ist von jedem Verantwortlichen zu führen, auf den einer der folgenden Punkte zutrifft.

- Das Unternehmen hat 250 oder mehr Mitarbeiter.
- Die Verarbeitung birgt ein mögliches Risiko für die betroffenen Personen.
- Die Verarbeitung erfolgt „*nicht nur gelegentlich*“.
- Es werden Daten besonderer Kategorien erhoben.

Das Verzeichnis muss kein reiner Formalakt sein, sondern ist in der Praxis vieler Unternehmen der Ausgangspunkt für die Recherche und Beschäftigung mit personenbezogenen Daten. Ein gut geführtes Verarbeitungsverzeichnis ist das zentrale Dokument zur Verwaltung relevanter Tätigkeiten und gibt den nötigen Überblick. Es kann als Leitfaden zur wiederkehrenden Prüfung der bestehenden Verarbeitungen

und als Muster für die Aufnahme neuer Verarbeitungsprozesse genutzt werden. Daher ist ein Verarbeitungsverzeichnis auch in Fällen empfehlenswert, in denen es nicht vorgeschrieben ist.

Unser Musterdokument im Anhang zeigt auszugsweise ein typisches Beispiel für ein Verarbeitungsverzeichnis.

Auf Anfrage einer Aufsichtsbehörde sind das Verarbeitungsverzeichnis und damit verbundene Dokumente (Liste der TOMs, IT-Sicherheitskonzept etc.) vorzulegen. Entgegen dem alten BDSG müssen Verarbeitungsverzeichnisse nicht mehr veröffentlicht werden.

Ein Auftragsverarbeiter muss ebenfalls ein Verarbeitungsverzeichnis pro Auftraggeber/Verantwortlichem führen. Darin sind zusätzlich der Name und die Kontaktdaten seines Auftraggebers/Verantwortlichen anzugeben. Dafür sind die folgenden Punkte nicht notwendig:

- Zwecke der Verarbeitung
- Kategorien der Daten und Personen
- Kategorien der Empfänger
- Löschfristen

Datenschutzfolgenabschätzung

Für jede Verarbeitung personenbezogener Daten ist nach Artikel 35 DSGVO das Risiko zu bewerten, das den betroffenen Personen durch Datenpannen oder Missbräuche entstehen kann. Die Risikoprüfung oder Schwellwertanalyse ist ein formloser Prozess, mit dem die Notwendigkeit einer Datenschutzfolgenabschätzung für einen Verarbeitungsvorgang geklärt wird. Eine Dokumentation der Risikoprüfung ist nach DSGVO nicht vorgeschrieben, in Deutschland wird sie jedoch von den Datenschutzbehörden gefordert, inklusive Angabe der wesentlichen Gründe.

Ergibt die Prüfung potenziell ein hohes Risiko, so ist eine Datenschutzfolgenabschätzung durchzuführen. Ausgehend vom ermittelten Risiko und der Eintrittswahrscheinlichkeit einer Datenpanne sind nun geeignete TOMs zu definieren, mit denen Risiko und Eintrittswahrscheinlichkeit reduziert werden. Die Maßnahmen werden dabei einer erneuten Analyse und Bewertung unterzogen. Ergibt sich dann immer noch ein mögliches hohes Risiko, ist die Datenschutzbehörde zu konsultieren.

Es gibt einige Leitfäden und Hilfsmittel zur Datenschutzfolgenabschätzung. So veröffentlichen die Aufsichtsbehörden Black- und Whitelists, in denen Verarbeitungstätigkeiten aufgeführt sind, für die eine DSFA erforderlich bzw. nicht erforderlich ist. Des Weiteren stellt die Nationale Datenschutzbehörde Frankreichs (CNIL) das PIA-Tool (PIA=Privacy Impact Assessment) zur Erstellung einer Datenschutzfolgenabschätzung zur Verfügung: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Weitere Informationen zur Datenschutzfolgenabschätzung können beim Bayrischen Landesamt für Datenschutzaufsicht eingesehen werden: https://www.lda.bayern.de/de/thema_dsfa.html

Datenschutzbeauftragter

Zu den Aufgaben eines Datenschutzbeauftragten (DSB) gehört weder die Umsetzung der DSGVO noch die Umsetzung der TOMs. Er überwacht die Einhaltung des Datenschutzes im Unternehmen, berät und schult die Mitarbeiter und arbeitet mit der Aufsichtsbehörde zusammen.

Für diese Aufgaben muss er Fachkenntnisse auf dem Gebiet des Datenschutzrechtes besitzen. Es gibt aktuell keine formell verpflichtende Qualifikation oder gar Zertifizierungen für einen Datenschutzbeauftragten.

Verantwortliche und Auftragsverarbeiter müssen nach den Regeln der DSGVO in folgenden Fällen einen Datenschutzbeauftragten benennen:

- Bei Behörden
- Kerntätigkeit beinhaltet umfangreiche, regelmäßige und systematische Überwachung von Personen
- Kerntätigkeit beinhaltet umfangreiche Verarbeitung von Daten besonderer Kategorien oder strafrechtlich relevanter Daten

Zusätzlich zu diesen Regeln gibt es in Deutschland weitere Gründe zur Benennung eines Datenschutzbeauftragten. Diese sind in § 38 BDSG definiert. Die beiden wichtigsten sind:

- Eine Datenschutzfolgenabschätzung ist erforderlich.
- Es sind mindestens 20 Personen (seit Herbst 2019) ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

Der Datenschutzkoordinator/-manager

Ein Datenschutzkoordinator oder Datenschutzmanager setzt die Anforderungen des Datenschutzes in einem Unternehmen praktisch um. Diese Rolle ist zwar nicht in der DSGVO definiert, kommt in der Praxis aber häufig vor.

Dabei handelt es sich oft um einen IT-Mitarbeiter, da er technische Kenntnisse im Bereich IT und Datenbanken hat und mit den Datenverarbeitungsprozessen des Unternehmens vertraut ist. Neben zahlreichen innerbetrieblichen Aufgaben schließt seine praktische Tätigkeit manchmal sogar die Vorbereitung und Prüfung der DSGVO-konformen Zusammenarbeit mit externen Dienstleistern und Softwarelieferanten ein.

Für diese zusätzlichen Aufgaben gibt es oft weder ein nennenswertes Budget noch eine entsprechende Fortbildung - und das obwohl der Mitarbeiter nicht nur die Aufgaben des Verantwortlichen, sondern nicht selten auch die des Datenschutzbeauftragten übernimmt.

Datenschutzberater

Neben dem Datenschutzbeauftragten und dem Datenschutzkoordinator gibt es noch eine dritte Rolle, den Datenschutzberater. An einen solchen externen Experten können sich Unternehmen mit fehlendem Knowhow im Datenschutz wenden. Neben der grundlegenden Beratung kann er laufend zur Bewertung neuer Sachlagen, technischer Möglichkeiten und Daten konsultiert werden.

Betrachtet man die Anzahl der Unternehmen, die keinen Datenschutzbeauftragten benennen müssen, und die Komplexität der Anforderungen, wird der Datenschutzberater immer wichtiger. Möglicherweise ist er in ein paar Jahren so selbstverständlich wie ein Steuerberater.

Datensicherheit

Datenschutz ist der Schutz von Rechten natürlicher Personen. Der technische und organisatorische Schutz von Daten wird hingegen unter dem Begriff “Datensicherheit” zusammengefasst. Er geht über die personenbezogenen Daten hinaus und betrifft alle Daten des Unternehmens.

Die DSGVO bezieht sich auf die Datensicherheit im Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“. Wir zitieren an dieser Stelle aus Artikel 25.1:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher

Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen[…].

Im englischen Original ist der Titel des Artikels die Maxime: "Data protection by design and by default".

„Data protection by design“ bezieht sich nicht nur auf die Verarbeitung der Daten, sondern auch auf die Planung, Beschaffung und Entwurf neuer Produkte und Dienstleistungen. Der Gesetzgeber fordert also schon bei der Beschaffung einer neuen Software, wie eines ERP- oder CRM-Systems, dass sie den Grundsätzen des Datenschutzes entspricht. Auf der anderen Seite sind die Hersteller angehalten, ihre Software und Dienstleistungen mit entsprechenden Funktionen und Sicherheitsmaßnahmen auszustatten.

„Data protection by default“ erwartet die datenschutzfreundlichste Konfiguration der Systeme als Standardkonfiguration. Verfügbare Sicherheitsmechanismen sollten immer aktiviert sein, außer sie werden durch eine bewusste und wohlbegründete Benutzeraktion deaktiviert. Das bezieht sich auf die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Diese Regelung zielt primär auf große Unternehmen, wie Facebook und Google, die ihr Geld mit Analyse und Handel von Daten verdienen. Diese Datenkraken haben seit Inkrafttreten der DSGVO reagiert und die Standardeinstellungen ihrer Systeme angepasst. Selbstverständlich gilt dieser Grundsatz für alle Entwickler und Anbieter von Anwendungen mit denen Daten verarbeitet werden.

Beispiel: Bei einer Access-Anwendung sind Entwicklerfunktionen wie Navigationsbereich, Ribbon, Shift-Taste etc. für alle Anwender deaktiviert.

Der zweite Artikel, der sich mit Datensicherheit beschäftigt, ist Artikel 32 „Sicherheit der Verarbeitung“. Dieser konkretisiert die Umsetzung der Datensicherheit und setzt die Analyse des notwendigen Schutzniveaus voraus.

Die Einstufung des Schutzbedarfs ist ein wiederkehrender Prozess. Bei jedem neuen Projekt oder bei Änderung der im Projekt verwendeten Datenkategorien muss das Schutzniveau der jeweiligen Daten neu bewertet werden.

Beispiel: Ein Datenbankentwickler erhält in einem bestehenden Projekt vom Kunden zusätzlich eine Tabelle, die Gesundheitsdaten enthält. In der DSGVO fallen Gesundheitsdaten unter die sogenannten „besonderen Kategorien“ und benötigen ein hohes Schutzniveau. Daher muss das Schutzniveau neu evaluiert und wahrscheinlich angehoben werden.

Eine Hilfestellung zur Ermittlung des passenden Schutzniveaus bietet die IHK-München: https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/Datensicherheit/

Die DSGVO nennt folgende technische und organisatorische Maßnahmen, mit denen die Sicherheit der Verarbeitung zu gewährleisten ist.

- Verschlüsseln
- Pseudonymisieren
- Vertraulichkeit und Integrität der Systeme und Dienste sicherstellen
- Verfügbarkeit und Belastbarkeit der Systeme und Dienste gewährleisten
- Schnelle Wiederherstellung der Systeme und Dienste ermöglichen
- Wirksamkeit der Maßnahmen prüfen und bewerten

Technische und Organisatorische Maßnahmen (TOMs)

Die DSGVO versteht unter Technischen und Organisatorischen Maßnahmen (TOMs) sowohl Maßnahmen im Rahmen eines IT-Sicherheitskonzeptes als auch im Rahmen des technischen Schutzes personenbezogener Daten in Dateien und Datenbanken.

Während in der DSGVO die TOMs nur abstrakt beschrieben werden, ist das deutsche Bundesdatenschutzgesetz konkreter und nennt in § 64 Abs. 3 folgende Punkte detailliert als TOMs. Diese Punkte gelten nach dem BDSG zwar für Polizei und Justiz, sind aber für Unternehmen ebenso zweckmäßig. Wir übernehmen die Punkte und ergänzen sie um erläuternde Stichworte.

- Zugangskontrolle
  Physischer Zugang zur IT-Infrastruktur, wie Sicherheitstüren, Schließ- und Alarmanlagen
- Datenträgerkontrolle
  Verhindern von unbefugtem Zugriff auf Datenträger, USB-Sticks, Festplatten, mobile Geräte etc. durch Maßnahmen wie Verschlüsselung und richtiges Löschen durch Aktenvernichter mit Crosscut und korrekte Festplattenvernichtung
- Übertragungskontrolle, Transportkontrolle
  Gesicherte und ggf. verschlüsselte Übertragung zu externen Schnittstellen wie Webservices, FTP-Server, VPN etc.
- Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle
  Zugriff nur für authentifizierte Benutzer auf Systeme und Daten in ihrem Zuständigkeitsbereich durch Passwort-Management, Chipkarten, Firewall etc., oder etwas lapidares wie Rechner sperren bei Abwesenheit ([Win]+[L])
- Eingabekontrolle
  Nachverfolgbarkeit der Erfassung, Änderung und Löschung von Daten
- Zuverlässigkeit, Datenintegrität, Verfügbarkeitskontrolle
  Fehlfunktionen schnell erkennen, USV, Brandmelder, Anti-Virensoftware
  Patch-Management bei Hardware, Routern, Mobile-Devices, Betriebssystemen, Anwendungen, Webseiten, Telefonanlagen, Druckern etc.
- Wiederherstellbarkeit
  räumlich getrennte und regelmäßig geprüfte Backups, ergänzt durch eine Desaster Recovery Strategie
- Auftragskontrolle
  Kontrolle von Auftragsverarbeitern und Verträgen
- Trennbarkeit
  Sicherstellen der getrennten Verarbeitung personenbezogener Daten, die zu unterschiedlichen Zwecken erhoben wurden

Hinweis:
Eine rein organisatorische und dennoch eine der wichtigsten Maßnahmen ist die Sensibilisierung und Schulung der Mitarbeiter. Uninformierte Mitarbeiter hebeln die meisten technischen Sicherheitsvorkehrungen aus – bewusst oder unbewusst.

Viele der genannten TOMs sollten im Rahmen eines bestehenden IT-Sicherheitskonzeptes bereits realisiert sein. Die DSGVO fügt hier nur einige neue Aspekte hinzu. Beispiele zu IT-Sicherheitskonzepten gibt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de

Datenschutzkonforme Softwareentwicklung

Die Bandbreite der Softwareentwicklung reicht von Formeln, die ein Mitarbeiter in einem Excel-Sheet einträgt, bis zur Erstellung von Individual- oder Standardsoftware durch einen externen Dienstleister. Überall in diesem weiten Spektrum sind die Grundsätze des Datenschutzes einzuhalten.

Viele offizielle Handlungsempfehlungen wie die des BSI beziehen sich auf die Erstellung von Software durch einen externen Dienstleister. Die Situation eines internen Entwicklers wird in der Regel nicht behandelt. In beiden Fällen sollte das Vorgehen bei der Softwareentwicklung mit den Verantwortlichen und ggf. dem Datenschutzbeauftragten abgestimmt werden.

Daten für Anforderungsanalysen / Konzepterstellung

Schon vor dem eigentlichen Start der Entwicklungsarbeit erhält der Entwickler oft für die Anforderungsanalyse und Angebotserstellung von bestehenden Kunden oder sogar von Interessenten personenbezogene Echtdaten.

Das ist aus Datenschutzgründen kritisch. Zum einen ist der Entwickler nun ebenso für die Sicherheit der Daten verantwortlich, zum anderen wird dem Grundsatz der Zweckbindung widersprochen, da der Absender die Daten sicherlich nicht zum Zweck der Softwareentwicklung durch einen Dritten erhoben hat. Außerdem fehlt ein entsprechender Vertrag zur Auftragsverarbeitung.

Selbst wenn bereits ein Auftragsverarbeitungsvertrag besteht, ist zunächst zu prüfen, ob die im Vertrag vereinbarten technischen und organisatorischen Maßnahmen den neu erhaltenen Daten genügen.

Wir empfehlen eine zeitnahe Rücksprache mit dem Absender der Daten, um die weitere und vor allem datenschutzkonforme Verarbeitung zu klären. Folgende Szenarien bzw. Vorgehensweisen sind denkbar:

- Anforderungsanalyse ohne personenbezogene Daten
  mit anonymisierten Daten, mit fiktiven Testdaten oder ohne Daten anhand der Struktur
- Anforderungsanalyse beim Kunden vor Ort
- Anforderungen mit dem Kunden per Fernwartung besprechen

Hinweis:
Auch personenbezogene Daten, die in Papierform übergeben werden, sind gemäß den Datenschutzregeln zu behandeln. Sie sind u.a. sicher aufzubewahren und bei Abschluss des Projekts zurückzugeben oder ordnungsgemäß zu entsorgen.

Daten in der Entwicklung

Die Weiterentwicklung von Software, wie auch die Fehlerbehebung direkt in der Produktivumgebung bringt ein erhöhtes Risiko mit sich. Durch Fehler des Entwicklers und durch unfertige Software können Daten verfälscht oder gelöscht werden. Aus diesem Grund sollte Softwareentwicklung nicht in der Produktivumgebung stattfinden.

Das Risiko der unabsichtlichen Veränderung oder Löschung lässt sich dadurch ausschließen, dass zur Softwareentwicklung eine Kopie der Daten in einer Testumgebung verwendet wird.

Diese Umgebung zum Entwickeln und Testen muss hinreichend isoliert sein, um keine verfälschenden Änderungen in der Produktivumgebung zu verursachen, z.B. Dateien löschen, PDFs im Rechnungsordner erzeugen, Exporte zu Schnittstellen. Zum Aufbau einer isolierten Testumgebung gehört meist, dass eigene Ordner für Importe, Exporte und Schnittstellen erstellt und diese in der Konfiguration der Testumgebung entsprechend eingetragen werden.

Im datenschutzrechtlichen Sinne spielt es keine Rolle, ob die verarbeiteten Daten direkt im Echtsystem vorliegen oder als Kopie. Sobald reale personenbezogene Daten verwendet werden, unterliegen diese Daten, der Entwicklungsprozess und die Entwicklungsumgebung den Anforderungen der DSGVO. Dies beinhaltet natürlich die Sicherheit der Verarbeitung, wie z.B. das verschlüsselte Speichern und Übertragen der Daten, sowie die sichere Aufbewahrung von Speichermedien (z.B. USB-Stick) und Backups. Ein großer Teil der Datenpannen ist mit den Kopien von Echtdaten in Entwicklungsumgebungen passiert.

Beispiel:
Ein Versicherungskonzern hat seine Produktivumgebung hervorragend abgesichert und einen unbefugten Zugriff darauf nahezu ausgeschlossen. Die interne Softwareentwicklung arbeitete jedoch mit einer Kopie dieser Daten. Diese Kopie war das leichte Ziel von Angreifern, da die dort verwendeten Sicherheitsmaßnahmen ungenügend waren.

Künstliche Testdaten hingegen unterliegen nicht der DSGVO. Daher sind sie einer Kopie der Echtdaten vorzuziehen. Das gilt insbesondere bei sensiblen Daten und der Übergabe der Daten an externe Entwickler. Die Verwendung von Echtdaten lässt sich allerdings nicht immer vermeiden, z.B. zur Analyse datenabhängiger Fehler.

Mit etwas Aufwand lassen sich Testdaten mit eigenen Routinen erzeugen, wodurch diese näher an den Erfordernissen des Projektes sind. Alternativ gibt es kommerzielle Tools zur Generierung von Testdaten.

Hinweis:
Personenbezogene Daten finden sich ebenso bei Prozessen rund um die Softwareentwicklung. Dazu gehören Fehlermeldungen, die per Screenshot an die Entwickler gesendet oder in Ticketsystemen gespeichert werden, Ablaufverfolgungen zur Performance-Optimierung u.a.

Datenbankanwendungen

Ziel und Zweck einer Datenbankanwendung ist das Verarbeiten und Speichern von Daten. Da sich in den meisten Fällen darunter personenbezogene Daten befinden, gilt die DSGVO auch für die Entwicklung solcher Anwendungen. Daraus ergeben sich einige neue Anforderungen an die Datenbankentwicklung.

Der Entwickler braucht hierzu fachliche Unterstützung durch den Auftraggeber bzw. dessen Datenschutzbeauftragten oder Datenschutzberater. Die Bewertung welche Daten zwingend benötigt werden, wie diese zu handhaben sind und welches Schutzniveau diese benötigen, kann er nicht allein vornehmen.

Klassifizieren von Daten

Um personenbezogene Daten in einer Datenbank bei Bedarf schnell lokalisieren zu können, empfiehlt sich eine Klassifizierung der Datenspalten aller Tabellen. Dabei sollte zwischen einfachen und besonderen personenbezogenen Daten unterschieden werden. Gründe für eine solche Lokalisierung gibt es viele: das Erfüllen der Auskunftspflicht, die geforderte Korrektur falscher Daten, das Löschen von Daten nach Zweckerfüllung oder auf Anforderung usw.

Gewährleisten der Integrität

Die Integrität bezieht sich u.a. auf das Verarbeiten korrekter Daten. Die Konsistenz der Daten lässt sich in Datenbanken durch die Funktionen der deklarativen Integrität, wie Fremdschlüsselbeziehungen, eindeutige Schlüssel etc. erreichen, eine prozedurale Prüfung der Datenintegrität durch Programmierung in VBA, T-SQL o.ä.

Protokollieren von Änderungen

Neuanlagen und Änderungen von personenbezogenen Daten sind mit Datum und Benutzernamen zu protokollieren. Ergänzend können die Werte vor und nach der Änderung in die Protokollierung aufgenommen werden.

Zweck der Protokollierung ist nicht nur die Nachverfolgbarkeit. Das protokollierte Änderungsdatum lässt sich auch zur Ermittlung der Daten verwenden, deren Aufbewahrungsfristen abgelaufen sind.

Minimieren von Daten

Der Grundsatz der Datenminimierung ist bereits beim Entwurf des Datenmodells zu beachten. Es sollte nur Daten vorsehen, die für die Geschäftsprozesse der Anwendung relevant sind.

Bereits erfasste Daten, die zur Zweckerfüllung nicht erforderlich waren, sind nach den Vorgaben der DSGVO zu löschen. Übliche Verdächtige: Geburtsdatum, Geschlecht, private Handynummern etc.

Löschen von Daten

Nachdem der Verarbeitungszweck erreicht ist oder wenn die Rechtsgrundlage nicht (mehr) vorhanden ist - in der Praxis oft nach Ablauf von gesetzlichen Aufbewahrungsfristen - müssen die Daten gelöscht oder anonymisiert werden. Ebenso sind Daten auf berechtigten Wunsch des Betroffenen zu löschen, wie auch unrichtige Daten, die nicht korrigiert werden können.

Für alle personenbezogene Daten sind Löschzeitpunkte festzulegen. Ausgangspunkt dafür kann das o.g. Änderungsdatum oder z.B. ein Rechnungsdatum sein. Dieses definierte Datum dient auch dazu, das Löschen von Datensätzen zu verhindern, die noch nicht gelöscht werden dürfen.

Dafür ist eine geeignete Funktionalität in der Anwendung vorzusehen oder zu ergänzen, um das Löschen unter Prüfung der Aufbewahrungsfristen und evtl. Sperrvermerke zu ermöglichen.

Anonymisieren von Daten

Eine Alternative zum Löschen von Daten ist das Anonymisieren. Anonymisieren bedeutet, dass die Daten keinen konkreten Personen zuzuordnen sind und diese Zuordnung auch nicht wiederhergestellt werden kann.

Anonyme Daten fallen nicht unter die DSGVO.

Die Anonymisierung kann verwendet werden, um die Daten für statistische Zwecke und Tests mit Datenmengen auch nach Ablauf der Löschfristen zu nutzen.

Sicherstellen der Vertraulichkeit

Um den Anforderungen an die Vertraulichkeit, z.B. durch eine Mandantenfähigkeit, fachliche Trennung oder Sichtbarkeit von Daten, gerecht zu werden, muss das Datenbankmodell abgestufte Zugriffsberechtigungen ermöglichen.

Mitarbeiter sollten nur auf Daten zugreifen können, die für Ihre Aufgaben erforderlich sind. Beispiele wären eine Zugriffberechtigung auf Abteilungsebene, Filialebene oder Mandantenfähigkeit.

Die Implementierung ist natürlich abhängig von den Anforderungen und den technischen Möglichkeiten der Entwicklungswerkzeuge. Die Bandbreite reicht von der physischen Trennung der Daten bis hin zur Gestaltung der Benutzeroberfläche.

Pseudonymisieren von Daten

Bei der Pseudonymisierung werden die Identifikationsmerkmale einer Person durch Kennzeichen ersetzt. Die Zuordnung der pseudonymisierten Daten zur tatsächlichen Person ist mithilfe des zugrundeliegenden Konzeptes bzw. Algorithmus jederzeit wieder möglich.

Aus diesem Grund sind Konzept und Algorithmus getrennt von den pseudonymisierten Daten aufzubewahren und durch geeignete TOMs vor einem unbefugten Zugriff zu schützen.

Die Pseudonymisierung ist lediglich ein Mittel, die Sicherheit der Verarbeitung zu erhöhen. Die Daten fallen weiterhin unter die DSGVO.

Verschlüsseln von Daten

Der Vorgang der Verschlüsselung ähnelt dem der Pseudonymisierung. Auch hier wird der ursprüngliche Inhalt durch andere Werte ersetzt, nur dass die Umwandlung durch einen Schlüssel erfolgt. Der Schlüssel verwandelt den Klartext in nicht lesbares Kauderwelsch.

Hinweis:
Das Umwandeln verschlüsselter Informationen in einen lesbaren Klartext ist ohne Schlüssel nicht mehr möglich. Deshalb sollten die verwendeten Schlüssel sorgsam verwaltet und gesichert werden. In der Regel läuft dies auf eine Schlüssel- oder Zertifikatsverwaltung hinaus.

Schnittstellen und externe Dateien

Datenbankanwendungen sind umzingelt von anderen Systemen und Dateien, wie importierte und exportierte CSV-Dateien, PDFs, Emails und Papierausdrucke. Werkzeuge wie Word Serienbriefe oder Excel-Pivot-Charts speichern eine von der ursprünglichen Datenbank unabhängige Kopie der Daten. Fehlerprotokolle und andere Logfiles beinhalten ggf. personenbezogene Daten. Zugriffsberechtigungen auf externe Systeme werden lesbar im Quellcode oder in Konfigurationsdateien gespeichert.

Bei allen diesen Beispielen ist die Sicherheit der Verarbeitung zu gewährleisten, z.B. durch beschränkte Zugriffsrechte oder die Verschlüsselung der Dateien vor der Datenübertragung. Auch die Zweckbindung ist zu berücksichtigen. Sofern sie denn überhaupt gegeben ist, sind die Daten nach Erreichen des Zwecks zu löschen.

Die Beispiele zeigen die Notwendigkeit einer Datenflussanalyse. Hierbei wird der Weg der Daten in die Datenbank und aus ihr heraus analysiert und dokumentiert.

Datenbank-Management-Systeme

Die Anforderungen lassen sich mit vielen Datenbankmanagementsystemen umsetzen. In den folgenden Kapiteln behandeln wir Microsoft Access und Microsoft SQL Server.

Microsoft Azure SQL Databases ist zwar eng verwandt mit dem SQL Server, aber insbesondere in Bezug auf Administration und Funktionsumfang gibt es einige Unterschiede. Dennoch treffen einige der im Kapitel “SQL Server” beschriebenen Punkte dort ebenfalls zu.

Ähnliches gilt für andere Datenbank Management Systeme, wie z.B. Oracle, MySQL und MariaDB. Allerdings sind dort die Terminologie und die Implementierungsansätze evtl. unterschiedlich.

Microsoft Access

Microsoft Access ist der weltweite Marktführer bei Desktopdatenbanken und Teil des meistverbreiteten Office Paketes. Das hat Auswirkungen beim Thema Datenschutz.

Access wird von Millionen Nutzern für vielfältige Aufgaben im kleineren bis mittleren Datenbankbereich verwendet, von einzelnen Personen zur Verwaltung privater Daten bis hin zu unternehmensrelevanten Daten in weltweit vernetzten Konzern-Abteilungen. Daher werden Unmengen von personenbezogenen Daten in Access-Datenbanken gespeichert und mit Access-Anwendungen verarbeitet. Die meisten Access-Entwickler sind nicht Teil von IT-Abteilungen, haben keine Budgets, Schulungen oder Tools für den Datenschutz.

Nimmt man als Maß Datenbank-Management-Systeme allgemein, so entsprechen einige Features bzw. deren Fehlen in Access nicht dem von der DSGVO für den Datenschutz verlangten "Stand der Technik".

Nimmt man hingegen Desktop-Datenbanksysteme als Maß oder vergleicht es mit anderen Desktop-Programmen wie Excel, in denen Unmengen von personenbezogenen Daten verarbeitet werden, fällt die Beurteilung anders aus. Diese Desktop-Tools haben ähnliche Datenschutzmechanismen, oft aber nicht die Vorteile von Access: flexible Datenbankfähigkeiten, RAD-Fähigkeiten d.h. einfache, schnelle, effiziente Programmierbarkeit, UI-Erstellung und -Anpassung.

Bei hohen Datenschutzanforderungen kann die Anwendung (Frontend) in Access bleiben und die Datenhaltung (Backend) auf einem Server-Datenbanksystem wie dem Microsoft SQL Server erfolgen, der mehr und bessere Features für den Datenschutz bietet.

Die DSGVO verlangt angemessene technische und organisatorische Maßnahmen. Die Angemessenheit ergibt sich aus dem Risiko, das den betroffenen Personen durch die Verarbeitung ihrer personenbezogenen Daten entstehen kann, sowie aus der Art und dem Umfang der Verarbeitungstätigkeiten. Unsere generelle Empfehlung ist daher, alle Maßnahmen zu treffen, die zu dieser Angemessenheit beitragen. Bei Access sind das alle gängigen Maßnahmen zur Absicherung der Daten, Oberflächen und Entwürfe.

Berechtigung auf Dateisystemebene

Da Microsoft Access eine dateibasierende Datenbank ist, sollten generell auf Dateisystemebene nur jene Benutzer Zugriff auf die entsprechenden Ordner bekommen, die auch tatsächlich mit der jeweiligen Access-Anwendung arbeiten. Allerdings erfordert die technische Implementierung von Access, dass diese Benutzer zum Ändern der Daten Schreib- und Löschrechte auf die Ordner mit den Datenbank-Dateien benötigen, damit Access die Sperrdatei (.ldb/.laccdb) erstellen und löschen kann.

Access-Anwendung über Terminal-Server bereitstellen

Access-Applikationen werden oft per Terminal-Server-Technologie wie Windows Terminal Services, Remote-Desktop oder Citrix-Varianten bereitgestellt. Neben Vorteilen bei der Performance und Administration erhöht das auch die Sicherheit von dateibasierenden Anwendungen wie Microsoft Access, da sich der direkte Zugriff auf Dateien über das Netzwerk einschränken lässt.

Datenbankkennwort verwenden

Access-Datenbanken mit personenbezogenen Daten können mit einem Datenbankkennwort verschlüsselt werden. Der Verschlüsselungsalgorithmus ist mit dem Wechsel des Datenbankformates von MDB zu ACCDB ab Access 2007 wesentlich sicherer geworden. Bei der Wahl des Kennwortes sind

die gängigen Regeln zur Vergabe eines sicheren Kennworts zu berücksichtigen: Mindestens 10 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen. Die bekannten Crack-Tools für Access-Dateien arbeiten beim ACCDB-Format mit Brute-Force-Angriffen und sind daher weniger effektiv gegen ein langes und komplexes Passwort.

Hinweis:
Die Kennwortlänge für Backend-Dateien ist in der Praxis auf 19 Zeichen begrenzt. Längere Kennwörter können zwar vergeben werden, der Zugriff auf verknüpfte Tabellen scheitert aber ab 20 Zeichen mit der Fehlermeldung "Kein zulässiges Kennwort".

Das Datenbankkennwort des Backends steht in der Connect-Eigenschaft von daraus verknüpften Tabellen im Klartext und ist somit leicht auslesbar. Daher ist es wichtig, auch das Frontend mit einem Datenbankkennwort zu verschlüsseln, um bereits verknüpfte Tabellen abzusichern. Auf diese Weise ist die Dateikette gegen Einbruchsversuche geschlossen.

Entwicklerfunktionen deaktivieren/ausblenden

Access bietet in seiner Programmoberfläche viele Funktionen, die für die Anwendungsentwicklung vorgesehen sind. Der Entwickler sollte eine abgesicherte Anwendungsoberfläche für die Benutzer erstellen, um den Zugriff auf diese Funktionen zu unterbinden.

- Standard-Ribbons mit Entwicklerfunktionen ausblenden und evtl. stattdessen benutzerdefinierte Ribbons verwenden
- Navigationsbereich ausblenden
- Spezialtasten deaktivieren
    - [F11] für das Einblenden des Navigationsbereiches
    - [F7] öffnet den Dialog der Rechtschreibkorrektur, der als Kennwort formatierte Texte im Klartext anzeigt
    - [STRG]+[G] öffnet den VBA-Editor und zeigt das Direktfenster an
    - [ALT]+[F11] öffnet den VBA-Editor
    - Umschalt-Taste (Shift) für das Umgehen der Startoptionen und des Autoexec-Makros

Benutzersteuerung implementieren

Benutzer lassen sich über Ihre Windows-Anmeldung identifizieren. Üblicherweise geschieht das in VBA mit API-Funktionen. Den einzelnen Benutzern kann dann innerhalb der Anwendung eine Berechtigungsstufe/gruppe zugewiesen werden, die ihnen nur Zugriff oder Aktualisierungsrechte auf die für Ihre Aufgaben erforderlichen Daten, Formulare und Berichte bzw. Steuerelemente gewährt.

Diese Form der Benutzersteuerung innerhalb der Access-Datei verbessert nur die Sicherheit innerhalb der Access-Applikation und unterbindet nicht den externen Zugriff über Excel, Access, ODBC etc. auf die Daten. Für legitime Benutzer der Anwendung lässt sich das nicht verhindern, für Andere genügt eine Einschränkung der Berechtigung auf Dateisystemebene.

ACCDE-Format und Runtime-Version verwenden

Diese Access-Features schränken v.a. unmittelbare Änderungen am Anwendungsdesign ein.

In einer ACCDE-Datei liegt der Quellcode nur in kompilierter Form vor und kann weder eingesehen noch geändert werden. Das Ändern von Modulen, Formularen und Berichten ist nicht möglich, aber Makros und vor allem Tabellen, Abfragen und die Daten sind ungeschützt.

Die Runtime-Version von Access blendet den Navigationsbereich aus, ebenso die für den Entwurf erforderlichen Befehle des Menübandes und versteckt die Entwurfsansichten der Objekte. Die Nutzung der Access-Applikation ist nur mit einer vom Entwickler erstellten Benutzeroberfläche möglich.

Diese beiden technischen Maßnahmen verhindern nicht den externen Zugriff auf die Daten.

Bewertung der Möglichkeiten in Access

Einige der bisher genannten Maßnahmen sind keine hohen Hürden für professionelle Angreifer, sehr wohl aber für die große Masse der Benutzer. Sie tragen dazu bei, die Zugänglichkeit der Daten und Entwürfe einzuschränken bzw. zu regeln und unterstützen damit auch die Fehlervermeidung bei der Datenverarbeitung.

Datenbank- und Anwendungsobjekte klassifizieren

Alle Teile von Datenbanken und Anwendungen zur Verarbeitung personenbezogener Daten sollten klassifiziert werden, um ihre Auffindbarkeit und Behandlung zu erleichtern und zu automatisieren. Access bietet hierzu keine eingebauten Tools oder Features. Es sind grundsätzlich zwei Methoden möglich:

1. Man verwendet bzw. missbraucht bestehende Features wie die Eigenschaft "Beschreibung" von Tabellen, Abfragen, Formularen und Berichten und hinterlegt dort ein Kürzel wie "DSGVO1", DSGVO5", das eine Kennzeichnung und Einstufung der Sensitivität der Daten darstellt. Eine andere Möglichkeit sind eigene Felder in den einzelnen Tabellen für diese beiden Aufgaben. Eine weitere Variante wäre die Verwendung von benutzerdefinierten DAO-Properties, die per VBA-Programmierung erstellt und befüllt werden. All diesen Methoden ist gemeinsam, dass die DSGVO-relevanten Merkmale direkt am jeweiligen Objekt sichtbar und zugänglich sind.
2. Man verwendet eine Metadatentabelle oder –Datenbank, um die Kennzeichnungen und Einstufungen der Datenbankobjekte vorzunehmen und zu speichern. Dieses Vorgehen fasst alle DGSVO-relevanten Informationen an einer zentralen Stelle zusammen.

Beide Vorgehensweisen ermöglichen automatisierte Auswertungen per VBA bzw. mit Abfragen. Separate Metadatentabellen sind einfacher zu verwalten und auszuwerten. Dagegen sind Klassifizierungen, die unmittelbar im oder am Objekt hängen, bei Änderungen am Objekt einfacher aktuell zu halten. Auch gehen diese Informationen bei einem Export oder Import des Objekts in eine andere Datenbank nicht verloren.

Datenänderungen protokollieren

Die Protokollierung kann man in Access mit Feldern für den ändernden Benutzer und das Änderungsdatum direkt in der jeweiligen datenhaltenden Tabelle umsetzen. Der Vorteil dieser Methode ist die Unmittelbarkeit. Das Änderungsdatum kann mit dem Standardwert Date() bzw. Now() automatisch in der Tabelle geschrieben werden. Für den Benutzernamen bietet Access keine solche einfache Lösung. Er muss per Programmierung hinter Formularen in die Datensätze geschrieben werden.

Eine andere Methode Änderungen nachverfolgbar zu machen, ist die Verwendung einer Meta-Protokollierungstabelle. Dafür ist wiederum Programmierung per VBA notwendig. Vorteile dieser Methode sind die Zentralisierung der Änderungsdaten und die Mehrstufigkeit. Alle Änderungen können protokolliert werden, nicht nur das Anlegen und die letzte Änderung, wie beim Protokollieren in der Datentabelle üblich. Thomas Möller bietet hierzu die fertige Komponente TM-AenderungsProtokoll an: https://team-moeller.de/?Downloads:TM-AenderungsProtokoll

Löschen, Anonymisieren und Minimieren von Daten

Zum Löschen von Datensätzen kann man in Access einen Satz Löschabfragen erstellen. Diese löschen ausgehend vom jeweils relevanten Rechnungsdatum oder letzten Änderungsdatum.

Als Alternative zum Löschen können die Daten auch anonymisiert werden. Die Anonymisierung von Daten lässt sich in Access nur durch eigene Konzepte und Entwicklung eigener Funktionen realisieren.

Oft kommt es vor, dass nur Teile der personenbezogenen Daten entfernt werden müssen, da sie nicht mehr zur Zweckerfüllung dienen. Diese Datenminimierung lässt sich in Access mit Aktualisierungsabfragen umsetzen.

Beispiel:
Die Zahlung eines Kunden wird von Kreditkarte auf Rechnung mit Lastschrift umgestellt. Die Kreditkartendaten im Kundenstamm sind nun nicht mehr nötig und können gelöscht werden.

TOMs dokumentieren und demonstrieren

Technisch-organisatorische Maßnahmen sind nach DSGVO zu dokumentieren. Das erfolgt hauptsächlich durch formelle Instrumente wie das Verarbeitungsverzeichnis und einen Katalog der TOMs. Es kann aber auch schon unmittelbar erfolgen, indem die o.a. Lösch- und Aktualisierungsabfragen sprechend benannt werden, z.B. qry_DSGVO_Rechnungsdaten_Gesetzliche_Aufbewahrungsfrist_10_Jahre_Loeschen.

Auf diese Weise wird nicht nur das DSGVO-Bewusstsein und der TOM-Charakter demonstriert und dokumentiert. Durch ein Präfix wie "qry_DSGVO" lassen sich diese Abfragen auch einfach zur regelmäßigen manuellen Ausführung auffinden oder die Ausführung automatisieren.

Erfüllen von Betroffenenrechten vorbereiten

Mit Access lassen sich die in Abschnitt “Rechte der Betroffenen” aufgeführten Rechte sehr gut und komfortabel vorbereiten und erfüllen.

Nehmen wir als Beispiel die umfangreichen Informationsrechte bzw. -pflichten. Die Anfragen der Betroffenen und damit verbundene Fristen können in Access verwaltet werden. Nach erfolgter Klassifizierung der personenbezogenen Daten (s.o.) lässt sich die Beantwortung weitgehend automatisieren. Dabei werden die relevanten Daten ermittelt, in Berichten dargestellt und z.B. als PDF-Datei per Email versendet.

Ähnliches gilt für die Bearbeitung der anderen Betroffenenrechte wie Löschanfragen, Korrekturen, Widersprüche und Einschränkungen.

Microsoft SQL Server

Anstelle eines Access-Backends lässt sich auch eine SQL Server Datenbank als Backend einer Access-Anwendung verwenden. Das Access-Frontend bleibt bei dieser Konstellation weitgehend erhalten, jedoch muss i.d.R. der Datenzugriff aus Gründen der Performance angepasst werden.

Es gibt mehrere Gründe zur Migration einer Access-Datenbank zu einer SQL Server-Datenbank. Im Zusammenhang mit Datenschutz und Datensicherheit sind hier insbesondere die Ausfallsicherheit und der Zugriffsschutz zu nennen. Schließlich gehören diese beiden zu der im Datenschutz geforderten Sicherheit der Verarbeitung, die – wie oben bereits beschrieben – durch technische und organisatorische Maßnahmen realisiert werden soll. Folgende Maßnahmen sind in der DSGVO aufgeführt:

- Sicherstellen der Integrität und Vertraulichkeit der Systeme und Dienste
- Pseudonymisieren und Verschlüsseln
- Gewährleisten der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit der Systeme
- Prüfen, Evaluieren und Bewerten der Wirksamkeit der getroffenen Maßnahmen

Diese Aufzählung beinhaltet mit Integrität, Vertraulichkeit und Verfügbarkeit die drei klassischen Ziele der Informationssicherheit. Bei genauerer Betrachtung der geforderten Maßnahmen verlangt die DSGVO hier nichts neues. Pseudonymisieren und Verschlüsseln sind als Mittel zur Gewährleistung der Vertraulichkeit anzusehen und die Belastbarkeit der Systeme und Dienste ist ein Bestandteil von deren Verfügbarkeit.

SQL Server bietet zu fast jedem dieser Ziele mehrere Möglichkeiten. Einige davon haben Auswirkungen auf den Datenzugriff von Access nach SQL Server. In solchen Fällen sind Änderungen in der Access-Anwendung erforderlich.

Integrität und Vertraulichkeit

Die Integrität bezieht sich u.a. auf das Verarbeiten korrekter Daten und das Nachverfolgen von Datenänderungen. Die Korrektheit der Daten lässt sich in SQL Server durch deklarative Integrität mittels Fremdschlüsseln, eindeutigen Schlüsseln etc. erreichen. Zum Zweck der prozeduralen Integritätsprüfung bietet SQL Server Gespeicherte Prozeduren, Sichten, Funktionen und Trigger.

Zum Nachverfolgen von Datenänderungen gibt es mehrere Möglichkeiten:

- Temporal Tables
  Automatisches Speichern älterer Versionen von Datensätzen in einer eigenen Tabelle
- Change Data Capture
  Sammeln der geänderten Daten eines Datensatzes zur weiteren Verarbeitung
- Change Tracking
  Sammeln der Information, welche Art von Änderung an einem Datensatz vorgenommen wurde
- OUTPUT
  Ergänzung für die Befehle INSERT, UPDATE und DELETE zur Ausgabe der hinzugefügten, geänderten oder gelöschten Werte
- Trigger
  Eigene Programmierung in einem After-Trigger zur Protokollierung der Änderungen

Vertraulichkeit ist der Schutz von Informationen vor unbefugtem Zugriff. Dieser Schutz kann durch klassische Berechtigungsvergaben erreicht werden, wie auch mit den von der DSGVO geforderten Maßnahmen Pseudonymisieren und Verschlüsseln.

Zugriffssteuerung

SQL Server bietet eine mehrstufige Sicherheitsarchitektur. Sie besteht aus der Zugriffssteuerung auf Ebene der SQL Server-Instanz und der Zugriffssteuerung für jede einzelne Datenbank.

Innerhalb der Datenbanken lässt sich die Rechtevergabe auf Datenbankobjekten, wie Tabellen, Sichten, Gespeicherte Prozeduren etc. über Datenbankrollen und Schemata realisieren. Ergänzend hierzu ist eine Zugriffssteuerung nach einer eigenen, definierten Geschäftslogik per “Row Level Security“ möglich sowie das Maskieren von Daten mittels ”Dynamic Data Masking”.

Pseudonymisieren

Die Pseudonymisierung von Daten kann man in SQL Server nur durch eigene Konzepte und Entwicklung eigener Funktionen realisieren.

Verschlüsseln

SQL Server bietet zur Verschlüsselung Zertifikate, symmetrische und asymmetrische Schlüssel. Diese Verschlüsselungsmethoden können miteinander kombiniert und auf verschiedenen Ebenen eingesetzt werden.

Mit speziellen T-SQL-Funktionen lassen sich beim UPDATE und INSERT Daten einzelner Spalten verschlüsseln und diese beim SELECT wieder entschlüsseln. Die eingesetzten Funktionen sind dabei abhängig von der verwendeten Verschlüsselungsmethode. Es gibt welche für den Einsatz von symmetrischen Schlüsseln, von asymmetrischen Schlüsseln und von Zertifikaten.

Die mit SQL Server 2016 eingeführte Funktion “Always Encrypted“ verfolgt einen anderen Ansatz. Der Schutz der verschlüsselten Daten geht hier über Zertifikate, die außerhalb des SQL Servers verwaltet werden. Benutzer mit Zugriff zum entsprechenden Zertifikat können den Klartext der Daten lesen, Benutzer ohne Zertifikat hingegen nicht. Auf diese Weise lässt sich z.B. vermeiden, dass ein Datenbankadministrator unerlaubt Daten liest oder ändert.

Das Ver- und Entschlüsseln beim Lesen und Schreiben der Daten erfolgt automatisch. Allerdings gibt es für diesen automatischen Datenzugriff einige Regeln zu beachten. Diese sind in der Dokumentation der jeweiligen SQL Server-Version umfassend beschrieben, ebenso die Limitationen im Zusammenspiel mit anderen Funktionen von SQL Server.

Mit “Transparent Data Encryption” (TDE) ist es auch möglich, die Dateien der Datenbank zu verschlüsseln. Microsoft spricht hier von der "Verschlüsselung ruhender Daten". Dies trifft es sehr gut, denn die Daten sind nur in den Datenbank-Dateien verschlüsselt. Sie werden beim Laden in den Arbeitsspeicher entschlüsselt und beim Schreiben in die Dateien wieder verschlüsselt. Dies erfolgt automatisch anhand eines Zertifikats. Die Übertragung der Daten von SQL Server zum Client und umgekehrt bleibt hierbei unverschlüsselt. Die TDE ist seit SQL Server 2019 in der Standard Edition verfügbar, in den vorherigen Versionen jedoch nur in der Enterprise Edition.

Neben den Daten und Datenbanken ist das Verschlüsseln der Datenbanksicherungen möglich. Dies erfolgt auf Basis eines Zertifikats. Ohne dieses Zertifikat lässt sich die Sicherung weder lesen noch wiederherstellen. Auf diese Weise sind die Sicherungsdateien vor Missbrauch gut geschützt.

Besondere Bedeutung hat die Transportverschlüsselung der Daten zwischen SQL Server und Client, wenn deren Kommunikation über öffentliche oder nicht gut gesicherte Netzwerke erfolgt. Dafür muss weder der Quellcode der Access-Applikation noch die SQL Server-Datenbank angepasst werden. Die Verschlüsselung der Netzwerkkommunikation wird durch eine entsprechende Konfiguration am SQL Server aktiviert und idealerweise mit den Optionen des verwendeten Treibers ergänzt. Danach erfolgt die Verschlüsselung beim Aufbau der Verbindung über SSL/TLS.

Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

Zur Gewährleistung der Verfügbarkeit und Belastbarkeit bietet SQL Server neben der Hochverfügbarkeit mit AlwaysOn die Möglichkeit der Datenbankspiegelung und des Transaktionsprotokollversands.

Diese Funktionen halten neben der aktuellen Datenbank eine zweite Version der Datenbank auf einem separaten SQL Server parat. Beim Ausfall eines SQL Servers wird auf den zweiten SQL Server umgeschaltet. Dies erfolgt je nach Konfiguration automatisch oder manuell.

SQL Server stellt zur Sicherung der Datenbanken eingebaute Funktionalität zur Verfügung. Die Vollsicherung erstellt eine komplette Sicherung der Datenbank, während sich mit der differenziellen Sicherung die Änderungen seit der letzten Vollsicherung sichern lassen. Eine Besonderheit ist die Transaktionsprotokollsicherung. Gut geplant verhindert sie im Falle eines Crashs größere Datenverluste. Je kürzer der Turnus einer Transaktionsprotokollsicherung, desto geringer der Datenverlust.

Die Brauchbarkeit von Datensicherungen muss regelmäßig überprüft werden. Nur mit intakten Datensicherungen ist das erfolgreiche Wiederherstellen der Daten möglich.

Prüfen, Evaluieren und Bewerten der Wirksamkeit

Der Aufwand dieser Anforderung sollte nicht unterschätzt werden. Daher ist es gut, dass sich mit SQL Server solche Prüfungen automatisieren lassen. Hierzu gibt es eine Vielzahl von Funktionen:

- Anmeldeüberwachung
  Protokollieren erfolgreicher und nicht erfolgreicher Anmeldungen
- Serverüberwachungsspezifikationen (SQL Server Level Auditing)
  Protokollieren von Änderungen an der Konfiguration einer SQL Server-Instanz
- Datenbank-Überwachungsspezifikation (Database Level Auditing)
  Protokollieren von Änderungen an der Konfiguration einer Datenbank
- Sicherheitsrisikobewertungen
  Analyse, Bewertung und Ausgabe der Sicherheitsrisiken einer Datenbank
- Richtlinienverwaltung
  Automatisiertes Überwachen konfigurierter Eigenschaften
- Erweiterte Ereignisse (Extended Events/XEvents)
  Benutzerdefinierte Protokollierung von Ereignissen

Klassifizieren und Betroffenenrechte

Neben der Sicherheit der Verarbeitung bietet SQL Server auch bei den organisatorischen Anforderungen zum Datenschutz Unterstützung. So lassen sich theoretisch personenbezogene Daten in Datenbanken mit der Funktion “Daten klassifizieren" (Classify Data) klassifizieren. Die Verwendung von Erweiterten Eigenschaften (Extended Properties) als Speicherort der Klassifizierung ist ein sinnvoller Ansatz. In der Praxis ist diese Art der Klassifizierung aufgrund der mangelhaften Benutzerfreundlichkeit leider nicht brauchbar.

Zum Erfüllen des Betroffenenrechts der Datenübertragbarkeit können die SQL Server Integration Services eingesetzt werden. Mit eigens erstellten SSIS-Paketen werden die Daten einer Person aus den unterschiedlichsten Datenquellen gelesen, in ein einheitliches Format transformiert und gespeichert. Fordert ein Betroffener das Recht auf Datenübertragbarkeit ein, ist lediglich das SSIS-Paket auszuführen.

Ebenso ist der Einsatz der SQL Server Reporting Services zur Erfüllung der Auskunftspflicht denkbar. Eigens definierte Berichte liefern die Informationen zu einer Anfrage.

Fazit

Datenschutz wird größtenteils als lästig empfunden - und ja, er bedeutet zusätzlichen Verwaltungsaufwand. Auf der anderen Seite sollte der bewusste und sorgsame Umgang mit Informationen über Personen eigentlich eine Selbstverständlichkeit sein. Die Wirklichkeit sah und sieht oft noch anders aus:

Neue Funktionen und bessere Auswertungsmöglichkeiten waren über viele Jahre die fast ausschließlichen Anforderungen an die Softwareentwicklung. Sichere Verarbeitung und IT-Security allgemein wurden mangels Zeit und Budget nicht in die Software integriert und im organisatorischen Umgang mit den Daten vernachlässigt. Die Folge sehen wir in den fast täglichen Meldungen zu Datenschutzverletzungen und Sicherheitspannen.

Die DSGVO richtet sich gegen diese Missstände. Sie zielt auf mehr Sicherheit bei der Verarbeitung und fordert mit "data protection by design and by default" genau uns Softwareentwickler zum Umdenken auf. Wir sind in der Lage, die Verarbeitungssicherheit in unseren Datenbankanwendungen zu erhöhen. Das macht nicht nur die Software qualitativ besser und professioneller, sondern stellt zunehmend einen Wettbewerbsvorteil dar. Die DSGVO fördert durch ihren Werbeeffekt und ihre Strafdrohungen das öffentliche Bewusstsein und höhere Budgets für den Datenschutz.

Um hier dabei zu sein, braucht man Fachwissen über Datenschutz, Datensicherheit und speziell die DSGVO. Das gehört mittlerweile zum Rüstzeug jedes Datenbankentwicklers. Dieses Whitepaper liefert einen Beitrag hierzu.

Anhänge

- Checkliste Bestandsaufnahme
- Verzeichnis der Verarbeitungstätigkeiten

Checkliste Bestandsaufnahme

Firma

- Firmenstruktur
    - Einzelunternehmen, Konzern, eigenständige Firma, Standorte, Filialen
- Ziel und Zweck des Unternehmens
    - IT-Systemhaus, Handel mit personenbezogenen Daten, Einzelhandel u.a.
- Mitarbeiter
    - Mitarbeiter im Innen- und Außendienst, Teilzeit-Mitarbeiter, Praktikanten, Studenten
- Datenschutz
    - Benannter Datenschutzbeauftragter
- Kunden
    - Kategorien der Kunden (Branche, Größenordnung)
    - Besonderheiten in Hinblick auf personenbezogene Daten (Sensible Daten, Massendaten)
    - Inland, EU, Nicht-EU
- Lieferanten
    - Kategorien der Lieferanten
    - Inland, EU, Nicht-EU
    - Externe Dienstleister, die für das Unternehmen Leistungen erbringen
      z.B. Steuerberater und Lohnverrechner, IT-Dienstleister, freie Handelsvertreter, Raumpfleger, Entsorger für Abfall wie auch für Vernichtung von Akten und Datenträgern, Marketing-Agentur, Druckerei, Lettershop

Gelände

Aufnahme aller Punkte mit Hinblick auf Zutritt und Zugang durch Mitarbeiter und Externe wie Kunden, Lieferanten, Dienstleister

- Gebäude
    - Zutritt, Türen, Schlüssel, biometrische Erkennung etc.
- Anmeldeverfahren
    - Besucherverzeichnis auf Papier mit Unterschrift, Namenskärtchen
- Räume
    - Büro, Werkhallen, Archive
    - Fahrstuhl mit Kartenzugang
    - Aktenschränke, Safes etc.

Beispiel:
Nach der Erfassung aller Orte kam noch eine Anmerkung der Sekretärin: “und der Chef sammelt alles, was ihn interessiert, in einem nicht versperrten Schrank hinter seinem Schreibtisch, Rechnungen, Kundenbriefe, Mitarbeiterauswertungen...”

Geräte und Maschinen

- Videoüberwachung und Fotografie
- Fahrzeuge
    - Ortungsdaten, Zeiterfassung, Fahrtenbuch, Navigationssysteme etc.

- IoT und Sensoren
- Sprachsteuerung
    - Alexa, Cortana, Siri & Co.
      bei Firmen-Smartphones wie auch privaten Smartphones der Mitarbeiter
- Shredder
- Medizinische Geräte mit Patientendaten

Hardware

- IT-Infrastruktur
    - Netzwerk, Server, Clients, Switche, Telefonanlagen etc.
    - Drucker und Scanner, insbesondere bei Leasinggeräten
- Mobile Geräte
    - Notebooks, Smartphones, Tablets
    - Bring your own device (BYOD) → Mischung private/berufliche/externe Daten und Kontrolle
- Externe Speichermedien
    - USB-Sticks, Festplatten, Backup-Bänder
- sonst. Gerätschaften mit potenziellen Sicherheitslücken
    - Smart-TV, Whiteboards, Surface Hub, IP-Kameras, Sensoren (IoT) etc.

Beispiel:
Aufgrund der Hitze im Sommer 2018 fiel die Klimaanlage im Serverraum aus. Die Server mussten in einer Hau-Ruck-Aktion in den Keller umziehen, da dort der kühlste Raum war.

Auf den ersten Blick mag dies nichts mit Datenschutz zu tun haben. Jedoch ist nach DSGVO die Verfügbarkeit und Betriebssicherheit zu gewährleisten. Fraglich ist, ob nach dem Umzug in den Keller die ebenfalls geforderte Vertraulichkeit durch einen Zutrittsschutz noch gegeben war.

Software

- Betriebssysteme
    - Server, Clients, Virtuelle Maschinen
- Konfigurationssoftware für Geräte wie Drucker, Scanner, Kamera etc.
- Office-Software
    - Inhalte der Dateien und Dokumente
    - Dokumentenmanagement-Software, Sharepoint
- Email-Software
    - Mailinhalte und Anhänge
    - Zentraler Mailserver und/oder Client-Software mit Offline-Funktion
    - Mail-Apps auf mobilen Geräten
- Mobile Device Management
    - Zentrale Steuerung mobiler Geräte, insbesondere der dort installierten Apps
    - Apps mit Standortbestimmung, Tracking-Funktionen etc.
- Kaufmännische Software
    - ERP, FiBu, CRM, Lohnbuchhaltung
- Technische Software
    - CAD, Maschinensteuerungen etc. (wegen Mitarbeiterdaten, Logins, Ansprechpartner)
- Tools

    - PDF-Drucker, ZIP-Programme und andere Tools mit möglichen Tracking-Funktionen
- Individual-Software
    - Datenbankanwendungen mit Access und SQL Server
    - Excel-Gebäude, Power Pivot, Power-BI
- Dateiablage
    - Transferordner
    - Daten-Exporte, Quell- und Zielverzeichnisse von Daten Import/Export

Beispiel:
Nach der Installation eines Remote-Zugangs für einen externen Entwickler (einer der Autoren) kam als letzter Punkt von der Konzern-IT: "und jetzt installieren Sie noch die App auf Ihrem Smartphone, mit der Ihnen das aktuell gültige Passwort gesendet wird."

Grundsätzlich ist gegen die Zusendung des Passworts nichts einzuwenden. Nur wurde hier von dem Externen verlangt, eine für ihn nicht prüfbare, fremde App auf seinem Smartphone zu installieren, wodurch die Vertraulichkeit und Integrität für die Daten auf seinem Smartphone nicht mehr gegeben wäre. Der Fernzugang wurde trotz Verdiensteinbußen dankend abgelehnt.

Internet und Dienste

- Firmenwebseiten
    - Online-Shop, Portal, Foren, Blog mit Kommentarfunktionen
- E-Mail-Provider und Web-Hosting
- Genutzte Webanwendungen
    - Google, Web-Mail
    - Online-Banking, Portale von Dienstleistern, Newsletter-Versender, insbesondere Websites mit Tracking-Tools
- Cloud-Dienste
    - Office 365, Azure, AWS, Google Docs
    - Dropbox, OneDrive etc.
- FTP-Server
- VPN-Zugänge
- Kommunikation
    - Telefon, Mobilfunk-Provider, DSL

Verzeichnis der Verarbeitungstätigkeiten

Verantwortlicher:
Andreas Maria Müller
Datengasse 42
17012 Dreiundzwanzig

Tel.: 0123/123456-0
E-Mail: info@ammdb.de
Web: www.ammdb.de

Geschäftsführer/Inhaber: Andreas Maria Müller

Datenschutzbeauftragter: kein DSB bestellt

Nr	Verarbeitungstätigkeit	Ansprechpartner	Version	Zwecke der Verarbeitung	Rechtsgrundlage	Kategorie betroffener Personen	Kategorie von personenbezogenen Daten	Besondere Datenkategorien nach Artikel 9	DSFA erforderlich	Profiling	Kategorie von Empfängern	Drittlandtransfer	Löschfristen	Speicherorte	Technisch-organisatorische Maßnahmen
1	**Kundenverwaltung**	Emma Stein 0000/7890123 es@ammdb.de	Verarbeitungs-tätigkeit eingeführt: 02.03.2018 Zuletzt geändert: 03.03.2019	Vertragserfüllung Vorvertragliche Maßnahmen Verwaltung der Stammdaten	Vertragserfüllung Vorvertragliche Maßnahmen	Kunden, Ansprechpartner, Mitarbeiter, Mitwirkende Geschäftspartner	Name, Adresse, E-Mail, Telefon, Steuernummer, Bankverbindung, Vertragstexte und Geschäftskorrespondenz Kundenkontakthistorie	keine	Nein	Nein	Banken, Steuerberater, Mitwirkende Geschäftspartner, E-Mail-Provider, Post- und Paketdienste	Datenaustausch per Dropbox nach USA (Dropbox auf der Liste der Mitglieder des Privacy Shield)	Max. 10 Jahre (Gesetzliche Aufbewahrungsfrist)	Datenbanken, E-Mail-Programm, Dokumenten-Dateien, Dropbox, Aktenordner, Archiv, CRM	Siehe Verzeichnis der ToMs und IT-Sicherheitskonzept
2	**Werbemaßnahmen zur Kundengewinnung und -bindung**	…	…	Werbemaßnahmen zur Kundenbindung	Wahrung berechtigter Interessen des Verantwortlichen	…	…	…	…	…	…	…	…	…	…
	…														

Hinweis:
Zusätzlich zu den Vorgaben aus Artikel 30 der DSGVO haben wir einige Spalten mit sinnvollen Zusatzinformationen aufgenommen.
- Version – um Änderungen nachverfolgen zu können
- Speicherorte – in welchen Büros, Lagerräumen oder welchen Programmen, Datenbanken etc. befinden sich die Daten
- Rechtsgrundlage – eine vom deutschen Bundesdatenschutzgesetz (BDSG) zusätzlich geforderte Information
- Profiling – eine vom BDSG zusätzlich geforderte Information
- DSFA erforderlich – dokumentiert, dass eine Risikobewertung und ggf. eine Datenschutzfolgenabschätzung durchgeführt wurde. Die Spalte könnte je nach Ergebnis einen Verweis auf die Dokumentation der Risikobewertung oder der DSFA enthalten.