DSGVO – Für Profis

Ein Überblick über die Datenschutzgrundverordnung

Hinweis: Dieser Beitrag ist keine Rechtsberatung. Bitte wenden Sie sich bei juristischen Fragen an einen fachkundigen Anwalt. Wir erheben kein Anspruch auf Vollständigkeit. Irrtümer vorbehalten.

I. Grundlegendes zur DSGVO

Was ist die DSGVO bzw. wann findet sie Anwendung?

Diese Schulung soll einen ersten Überblick über die Umsetzung lt. DSGVO geben.

Die DSGVO hat grundsätzlich ein Ziel: Die Grundrechte und Grundfreiheiten natürlicher Personen, und insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen.

Sie soll:

- einen globalen Datenschutzstandard setzen
- Verbot von “Forum Shopping” (keine Chance, dass Ihre Daten in Länder mit niedrigerem Datenschutzniveau übermittelt werden) ermöglichen.
- eine bessere Kooperation mit Datenschutzbehörden innerhalb Europas fördern

Die DSGVO findet grundsätzlich immer Anwendung. Die einzige Ausnahme ist, wenn spezielle nationale oder EU-Gesetze dem Gegenüberstehen. Spezielle Regelungen sind z. B. TMG, TKG and UWG.

Die Verpflichtungen aus der DSGVO gab es auch schon früher, zu Zeiten des Bundesdatenschutzgesetzes[1] (BDSG). Die Standards und Strafen wurden erhöht, da die alten Regelungen auf Grund der rasant veränderten technischen Möglichkeiten und den immensen Datenskandalen nicht mehr ausreichend waren.

Die Umsetzung der DSGVO kann, je nach Unternehmensgröße, unterschiedlich aufwendig sein. Allgemein sollte man im Zuge der Evaluierungen, die bestehende Handhabung innerhalb des Unternehmens hinterfragen.

Rechtsgrundlagen Verarbeitung

Die Verarbeitung von personenbezogenen Daten darf nur in einem bestimmten Rahmen erfolgen. Es gibt sechs verschiedene Grundlagen, wobei Ausnahmen möglich sind.

- Einwilligung zur Verarbeitung, zweckgebunden
- Vertragliche bzw. vorvertragliche Maßnahmen
- Erfüllung einer rechtlichen Verpflichtung
- Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
- Wahrung der berechtigen Interessen des Verantwortlichen oder eines Dritten, ausgenommen, dass die Interessen oder Rechte einer betroffenen Person überwiegen

[1] BDSG - https://www.lda.bayern.de/media/info_datengeheimnis.pdf

Was sind personenbezogenen Daten?

Personenbezogene Daten sind Daten, die einer Person zuzuordnen sind, z. B.

- Name
- Alter und Geburtstag
- Adresse, E-Mail Adresse
- Telefonnummer
- IP-Adresse
- sonstige Daten, die eine Person eindeutig identifizierbar machen

Für sensible Daten gibt es besondere Schutzbestimmungen, damit sind unter anderem

- Strafrechtliche Informationen
- Patientendaten
- Sexuelle Orientierung
- Politische Ansichten, Parteizugehörigkeit
- Religion/Weltanschauung
- Bankdaten

gemeint. Für diese Kategorien ist zum Beispiel Profiling verboten (§9, DSGVO). Es gibt jedoch auch hier Ausnahmen.

Rechte der betroffenen Personen

Um sicherzustellen, dass Daten auch ordnungsgemäß gehandhabt werden, haben Betroffene diverse Rechte. Dazu zählen unter anderem:

- Löschung/Vergessen werden: Betroffene können jederzeit die Löschung Ihrer Daten verlangen, vorausgesetzt kein wichtigere Grund steht dem entgegen.
- Einschränkung: Betroffene dürfen in bestimmten Fällen die Einschränkung der Verarbeitung fordern.
- Datenberichtigung/Übertragbarkeit: Betroffene können ihre hinterlegten Daten jederzeit berichtigen lassen oder eine maschinenlesbare Kopie eben jener atz veranfordern.
- Widerspruchsrecht: Betroffene können Widerspruch gegen die Datenverarbeitung erheben, vorausgesetzt, diese ist nicht unbedingt notwendig zur Vertragserfüllung
- Auskunftsrecht: Betroffene müssen über alle gespeicherten Daten Auskunft erhalten, sowie über die Herkunft.
- Informationspflicht: Der Betroffene muss vorab über die Verarbeitung informiert werden, z.B. bei Abschluss eines Vertrages oder relevanten Änderungen in der Handhabung

Das involvierte Unternehmen muss diese Rechte respektieren und reagieren. Besonders das “Recht auf Vergessenwerden” ist ein essentieller Teil der DSGVO. Die betroffene Person soll Herr der Daten bleiben. Das Ziel ist, dass personenbezogene Daten nicht beliebig lange gespeichert werden, sondern nur solange sie relevant sind.

Ein weiteres, wichtiges Recht ist die Datenportabilität. Das erlaubt dem Betroffenen eine Kopie seiner Daten anzufordern.

Diese Kopie muss in einem strukturierten, gängigen und maschinenlesbaren Format sein. Strukturiert bedeutet im Datenbankformat (XML, SQLite etc.).

Was ist der Unterschied zwischen Datensicherheit und Datenschutz?

Datenschutz und IT-Sicherheit agieren im Idealfall wie Ying und Yang, ohne IT-Sicherheit ist Datenschutz schwer umsetzbar. Viele große Unternehmen (z. B. Facebook und Google) sichern ihre Systeme gut ab, verdienen aber ihr Geld mit dem Verwerten von Daten für personalisierte Werbung. Der Datenschutz steht hier also an zweiter Stelle. Wichtig ist, dass IT-Geräte, die personenbezogenen Daten speichern, auch entsprechend technisch abgesichert sind. Nur so ist die Privatsphäre gewährleistet.

Je nach Art bzw. Kategorien der Daten müssen angemessene technische und organisatorische Maßnahmen getroffen werden, um diese entsprechend zu schützen.

Hier gibt es verschiedene Kategorien n. TOM gemäß Anlage § 9 BDSG

- **Zugangskontrolle**: Kein Zugang für Unbefugte
- **Zutrittskontrolle**: Kein Zutritt für Unbefugte
- **Speicherkontrolle**: Systeme dürfen nur von autorisierten Personen benutzt werden (z. B. Login und Passwort)
- **Benutzerkontrolle**: Nutzung einer Autorisierungsstruktur (z. B. Nutzerrechte)
- **Übertragungskontrolle**: Keine Veränderung, Inspektion, Löschung von Daten während ihrer elektronischen Übermittlung oder -speicherung
- **Eingabekontrolle**: Es muss nachvollziehbar sein, wann und von wem personenbezogene Daten eingegeben oder verarbeitet/gelöscht wurden
- **Übertragungs-/Weitergabekontrolle**: Gewährleistung, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
- **Verfügbarkeit**: Personenbezogene Daten müssen vor (vorsätzlicher oder nicht-vorsätzlicher) Beschädigung oder vor Verlust gesichert sein (Backup)
- **Trennbarkeit**: Personenbezogene Daten, die für verschiedene Zwecke gesammelt werden, müssen auch getrennt verarbeitet werden.

BYOD

All das heißt natürlich auch, dass man vorsichtig mit Kundendaten umgehen sollte. BYOD (Bring your own device – Bring dein eigenes Gerät mit) ist ein hohes Risiko für den Datenschutz. BYOD heißt, dass Mitarbeiter ihre privaten Geräte, wie Smartphones, zu Geschäftszwecken nutzen.

Gründe gegen BYOD sind u.a.

- Abfangen von Informationen/Identitätsdiebstahl, durch Schadsoftware, Tracking o.ä.
- Botnetaktivitäten/Missbrauch
- Stehlen von Geschäftsgeheimnissen/Stehlen von Knowhow
- Wegen mangelnder Sicherheitseinstellungen Weiterleiten von Informationen, z.B. Adressbuchdaten, an Trackingdienste, Werbeunternehmen oder andere Dritte.

Wer einen ausführlicheren Überblick braucht, warum "Bring your own device" schnell schädlich werden kann, sollte sich die Reihe des Kuketz Blog: Android ohne Google[1] ansehen.

Was bedeutet das bei der täglichen Arbeit?

Jeder der Daten verarbeitet, muss sicherstellen, dass er diese unter den oben genannten Prinzipien tut. Aufgrund der unterschiedlichen Gesetzeslagen zwischen den verschiedenen Ländern (außerhalb der EU) unterscheiden sich die Datenschutzgesetze enorm – oder sind überhaupt nicht vorhanden.

Es besteht jedoch die Möglichkeit, dass die EU-Institutionen zusätzliche Regelungen diesbezüglich erlassen. Der Effekt einer solchen Regelung ist, dass personenbezogene Daten außerhalb der EU[2] (und des EWR) in das Drittland fließen können, ohne dass weitere Maßnahmen notwendig sind. Anders ausgedrückt, Daten, die dorthin übermittelt werden, werden genauso behandelt wie Daten innerhalb der EU.

Die Europäische Kommission hat bis jetzt Andorra, Argentinien, Kanada (kommerz. Institutionen), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Japan, Uruguay als Länder mit adäquaten Datenschutz[3] identifiziert. Derzeit werden weitere Gespräche mit Südkorea geführt.

Im Allgemeinen ist der Aufwand zu Einführung der DSGVO einmalig und dann fortlaufend, wenn sich Änderungen in der Datenverarbeitung ergeben.

Problematik USA

Die USA haben bis jetzt keinen adäquaten Datenschutzstandard.

Im Gegensatz zur EU ist der Datenschutz in den USA[4] nicht umfassend reguliert. Es gibt stattdessen industriespezifische Regulierungen. Viele dieser Regulierungen basieren rein auf freiwilligen Verpflichtungen. Firmen sind dann an industriespezifische Privatsphäreregelungen gebunden, welche die Sicherheit der personenbezogenen Daten, die sie speichern, garantieren sollen.

---

[1] https://www.kuketz-blog.de/your-phone-your-data-teil1/

[2] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[3] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_de

[4] https://www.datenschutz.org/usa/

Das in den USA angewandte Prinzip erlaubt den Unternehmen ihr Datenschutzlevel quasi selbst festzulegen.

Wenn diese jedoch ihre eigenen Regelungen verletzen, wird das als eine täuschende und unfaire Praxis angesehen und natürlich mit rechtlichen Konsequenzen bestraft.

Zusätzlich zu dem niedrigen Datenschutzniveau in den USA ist der extensive Datenzugriff durch die US-Behörden und die Weitergabe der Daten an Dritte problematisch für den Datenaustausch mit der EU.

Nach aktuellen Medienberichten denken die USA im Moment über ihre eigene DSGVO nach einem europäischen Standard nach. Derzeit ist es jedoch noch schwierig, datenschutzkonform Daten in die USA zu übermitteln. Tatsächlich war das Privacy Shield Abkommen, der Nachfolger des Safe Harbor Abkommens, dafür da, um die entsprechenden Rahmenbedingungen für einen sicheren Datenaustausch zwischen Europa und den USA zu schaffen.

Demnach ist eine Datenübermittlung auch nur in Länder erlaubt, die ein "angemessenes Schutzniveau" (Artikel 45) haben. Aus Sicht des europäischen Parlaments[1] ist dies für die USA derzeit nicht vorhanden.

Als Beispiel: Der Skandal um Facebook und Cambridge Analytica zeigte, wie porös das Privacy Shield in Wirklichkeit ist. Mitglieder des europäischen Parlaments bemerkten, dass Unternehmen zwar die Privacy Shield Verträge unterzeichneten, diese dann jedoch verletzten. Das Endergebnis ist nun der Versuch solche Datentransfers vollständig zu unterbinden. Derzeit ist der Stand der Verhandlungen nicht bekannt.

Außerdem ist der Cloud Act für das europäische Parlament problematisch. Dieser erlaubt US-Sicherheitsbehörden auf Daten, die außerhalb der USA von US-Firmen gespeichert werden, zuzugreifen. Die Zukunft des legalen oder cross-company Datentransfer zwischen der europäischen Union und den USA ist immer noch unklar.

Unglücklicherweise sind viele Technikriesen in den USA angesiedelt und übermitteln und speichern ihre Daten auf US-Servern. Wenn es keinen Vertrag zwischen der US-Firma und der EU-Firma gibt, sollte der Datentransfer unterbunden werden. Der US-Markt reagiert inzwischen ebenfalls auf die DSGVO und hat den Zugang zu einigen Nachrichtenportalen für die europäischen Besucher gesperrt.

Auftragsverarbeitungsvertrag

Ein Auftragsverarbeitungsvertrag (AVV) ist immer dann notwendig, wenn ein Dritter in Kontakt mit personenbezogenen Daten kommt. Dies kann z.B. durch Beauftragung eines Steuerberaters zur Abwicklung der Buchhaltung passieren.

Grundsätzlich sollte der Auftragsverarbeitungsvertrag spezifische Regelungen zur Handhabung, Verschwiegenheit usw. beinhalten.

---

[1] http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps

Die Einhaltung sollte überprüft und keine Daten an Dritte übermittelt werden, ohne einen eben solchen Vertrag. Bei Verstößen, drohen harte Sanktionen.

II. Der Datenschutzbeauftragte

Firmen mit mehr als 10 Mitarbeitern (egal ob interne oder externe), die automatisiert personenbezogene Daten verarbeiten, benötigen einen Datenschutzbeauftragten. Ebenso benötigt, unabhängig davon, jedes Unternehmen, dass sensible Daten verarbeitet oder solche, die ein Risiko für die Rechte und Freiheiten einer Person darstellen, einen Datenschutzbeauftragten. Eine Unternehmensgruppe kann bspw. einen gemeinsamen Datenschutzbeauftragten ernennen, sofern dieser von allen Niederlassungen einfach erreichbar ist.

Wenn Arbeitnehmer oder das Unternehmen Fragen bezüglich des Datenschutzes haben, oder neue Software einführen möchten, müssen sie den Datenschutzbeauftragten konsultieren. Des weiteren muss alles mitgeteilt werden, die sich in irgendeiner Weise mit der Verarbeitung von personenbezogenen Daten auseinandersetzen.

Der Datenschutzbeauftragte (DSB) muss berufliche Qualifikationen und entsprechendes Fachwissen vorweisen können. Die Fähigkeit zur Ausführung der Tätigkeit muss gegeben sein. Er ist ebenso auf Verschwiegenheit verpflichtet und berichtet in der Regel der höchsten Management-Ebene. Andere Tätigkeiten innerhalb des Unternehmens dürfen ausgeführt werden, sofern kein Interessenkonflikt besteht.

Das Unternehmen wiederum muss dem DSB alle notwendigen Ressourcen und Zugriffe gewähren, es darf also die Arbeit nicht behindern. Im Gegenzug berät und informiert der DSB das Unternehmen. Er überwacht außerdem die Einhaltung der entsprechenden rechtlichen Vorschriften und fungiert als Anlaufstelle für die Datenschutzbehörde.

Wer kontrolliert die Einhaltung des Datenschutzes?

Jedes private Unternehmen (außer die Telekommunikations- und Postunternehmen) unterstehen den jeweiligen Datenschutzbehörden der einzelnen Bundesländer.

Post/Telekommunikationsanbieter sind beim Bundesdatenschutzbeauftragten angesiedelt.

Sanktionen

Es ist in der DGSVO geregelt, dass die Strafen effektiv, angemessen und abschreckend sein müssen und zwar in jedem individuellen Fall. Um festzustellen, wann und in welcher Höhe Sanktionen erhoben werden, haben die Aufsichtsbehörden eine Liste von vordefinierten Kriterien, welche in diese Entscheidung mit einfließen. Für schwerwiegenden Verstöße, welche in der DSGVO unter Art. 83 (5) gelistet sind,

kann die Strafe bis zu 20 Mio. Euro oder bis zu 4% des weltweiten jährlichen Umsatzes betragen, je nachdem, welcher der Beträge höher ist.

Beispiel: Wenn Unternehmen ABC die Datenschutzgrundverordnung nicht respektiert und einhält, muss das Unternehmen bis zu 4% des weltweiten jährlichen Umsatzes o. 20 Mio EUR bezahlen.Das Unternehmen hat z. B. 2 Milliarden Euro weltweiter jährlicher Umsatz in 2018, davon 4% Strafe → 80 000 000 Euro. Die Strafe wäre 80 Mio Euro (höchste Strafe)!

Genau wegen dieser hohen Strafen wollen Unternehmer sicherstellen, dass die Arbeitnehmer wissen, wie man mit Daten richtig umgeht. Deswegen müssen die Arbeitnehmer eine Verpflichtung auf das Datenschutzgeheimnis unterzeichnen und entsprechende Aufklärung erhalten. Natürlich muss dann auch vom Arbeitgeber sichergestellt werden, dass die Arbeitnehmer sich das Wissen aneignen (wie z. B. mit Schulungen), um einen Nachweis zu haben.

Denn wenn der Arbeitnehmer die aktuellen Datenschutzregelungen bzw. gesetzten Firmenstandards nicht einhält, muss der Arbeitnehmer ggf. für den Missbrauch zahlen (Verpflichtung auf das Datengeheimnis).

Auch soll sichergestellt werden, dass die Dienstleister/Auftragsverarbeiter hohe Datenschutzstandards setzen und diese natürlich auch umsetzen. Dafür brauchen Auftragsverarbeiter (Dienstleister) Auftragsverarbeitungsverträge. Diese Verträge beinhalten zahlreiche Informationen, wie die Daten verarbeitet werden, welche Daten verarbeitet werden, wo sie gespeichert sind und wer dafür verantwortlich ist.

Meldungen von Verletzungen des Schutzes an die Aufsichtsbehörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Eine Meldung muss lt. DSGVO folgendes beinhalten:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten beinhalten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

- Eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
- Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.

Es empfiehlt sich, vorab Dokumente auszuarbeiten, die im Falle des Falles nur noch ausgefüllt werden müssen. Entsprechende Vorlagen erhalten Sie auf den Webseiten der Aufsichtsbehörden oder von Ihrem Rechtsbeistand.

III. Einführung der DSGVO – Wo anfangen?

Am besten fängt man mit dem Verfahrensverzeichnis an, das gibt eine gute Übersicht über den derzeitigen IST-Zustand. Von dort aus kann man später viel einfacher strukturiert weiterarbeiten. Das Verfahrensverzeichnis sollte in regelmäßigen Intervallen geprüft und aktuell gehalten werden. Aktives Mitdenken aller Arbeitnehmer, die neue Prozesse mit personenbezogenen Daten oder neue Software melden, ist eine gute Voraussetzung.

Als Erstes gilt, erst einmal alle Verfahren zu sammeln, in denen Sie oder Ihre Kollegen in irgendeiner Weise in Kontakt mit Daten von realen Personen kommen. Das ist z. B. die Abrechnung, Personalmanagement, Marketing usw.

Das Verfahrensverzeichnis listet alle “Prozesse” auf, in denen Daten gesammelt, verarbeitet oder weitergeleitet werden.

Der Inhalt ist in Artikel 30 der DSGVO festgelegt:

- Name und Kontaktinformation der verantwortlichen Person
- Zweck der Verarbeitung (WARUM-Frage)
- Welche Personengruppen betroffen sind und welche Daten
- Wer diese Daten empfängt (interne, externe, Drittländer?)
- Übermittlung in Drittländer (ist das rechtlich abgesichert?)
- Löschfristen (wenn möglich)
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (wenn möglich)

Beispiel: Sie sind verantwortlich für die Abrechnungen Ihrer Arbeitnehmer. Das ist ein Prozess, welcher dokumentiert werden muss. Wenn Sie jedoch ein Dienstleister sind, der die Abrechnungen für seine Kunden macht, dann muss hier ein Auftragsverarbeitungsvertrag zwischen Ihnen und ihrem Kundenunternehmen geschlossen werden.

Ein Verfahrensverzeichnis könnte wie folgt aussehen:

- Name des Prozesses
- Verarbeiter
- Zeitpunkt der Datenerfassung
- Name, Telefonnummer, E-mail Adresse der verantwortlichen Personen
- Beschreibung des Prozesses/Zwecks der Datenerhebung
- Betroffene Gruppen/betroffene Daten
- Empfänger der Daten/Empfänger der Daten in einem Drittland
- Beschreibung der IT-Sicherheit/Sicherheitsregelungen/Datenschutzbestimmungen/-vorkehrungen im Drittland
- Löschfristen
- Beschreibung der IT-Sicherheit & der physischen Sicherheit der Daten

In welcher Form das Verarbeitungsverzeichnis geführt wird, ist Ihnen überlassen, es muss nur einfach zugänglich sein. (bspw. Tabelle, Textdokument)

IV. Datenschutzfolgeabschätzung – DSFA

Sobald die Prozesse aufgelistet wurden, folgt eine Datenschutzfolgeabschätzung, welche bei vielen Prozessen, bei denen personenbezogene Daten verarbeitet werden. durchgeführt und dokumentiert werden muss. Die DSFA nach Art. 35 DSGVO dient dem Zweck, bereits in einem frühen Stadium bei der Neueinführung von Verarbeitungsvorgängen die voraussichtlichen Risiken für die persönlichen Rechte und Freiheiten betroffener Personen zu identifizieren. Gleiches gilt bei allen wesentlichen Änderungen an Datenverarbeitungsvorgängen oder -systemen.

Wann benötigt man eine Datenschutzfolgeabschätzung (DSFA)?

In den nachfolgenden Absätzen gehen wir näher auf diese Thematik ein.

Nach Art. 35 Paragraph 1 DSGVO: "Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.”

Art. 35 (3) der DSGVO listet Beispiele auf, wann eine DSFA notwendig ist:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits

als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Es gibt jedoch auch Ausnahmen, so kann die zuständige Behörde eine Art „Whitelist“ für Datenverarbeitungen veröffentlichen die von dieser Pflicht ausgenommen sind. Außerdem ist es möglich von einer vollständigen DSFA abzusehen, wenn voraussichtlich kein hohes Risiko besteht. Für weitere Informationen diesbezüglich wenden Sie sich bitte an einen Rechtsbeistand und/oder Ihren Datenschutzbeauftragten.

Risikobeurteilung

Eine Datenschutzfolgeabschätzung ist notwendig, wenn die Risikobeurteilung Anlass zur Sorge gibt, dass die Datenverarbeitung ein hohes Risiko für diejenigen birgt, deren Daten verarbeitet werden. Das datenschutzrechtliche Risiko der Betroffenen, sprich der Personen, deren Daten verarbeitet werden (kein Risiko für die Firma), muss auf Basis von objektiven Kriterien (Herkunft, Umstände und Zweck der Verarbeitung) geschehen:

- Die Wahrscheinlichkeit des Eintreffens (Risikoquelle, Angreifer und jeder dadurch entstandene Schaden)
- nach der Schwere des Schadens (nicht kritisch, kritisch, sehr kritisch)
- Für verschiedene Verarbeitungen ist eine Schätzung ausreichend, wenn manche Prozesse ein ähnlich hohes Risiko haben.

In der Vorabeinschätzung ist natürlich auch wichtig, um welche Art der Daten es sich handelt (Kundendaten, Arbeitnehmerdaten, Steuerdaten, Gesundheitsdaten etc.).

Das sind die notwendigen Schritte für die Risikobeurteilung. Artikel 29 gibt uns auch Kriterien an die Hand, ob eine Datenschutzfolgeabschätzung notwendig ist. Normalerweise ist das der Fall, wenn zwei der folgenden Punkte erfüllt sind:

Allgemeines (z.B. Scoring oder Profiling)

- Automatisierte Entscheidungsfindung mit Rechtswirkung
- Systematische Überwachung (z. B. den Arbeitsplatz)
- Sensible Daten
- Datenverarbeitung in großem Umfang
- Abgleichen oder Zusammenführen von Datensätzen
- Daten von schutzbedürftigen Betroffenen (z. B. Kindern, Arbeitnehmern)
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen (z. B. biometrische Identifikation)

- Die betroffenen Personen könnten an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert werden.

Schaden

Eine Personen kann physischen, materiellen oder immateriellen Schaden durch Datenverarbeitung erleiden. Bei Einführung der geplanten Software/Applikation muss klargestellt sein, welche Art Schaden für Personen hierbei entstehen kann:

- Diskriminierung
- Identitätsdiebstahl
- Schaden der Reputation
- Finanzieller Schaden / Verlust der eigenen Daten
- Profilerstellung inkl. Standortdaten

Wie führt man eine DSFA durch?

1. Definieren Sie einen Bewertungsbereich (Beschreibung der Prozessoe, inklusive Datenflüsse und Zweck der Verarbeitung)
2. Identifizieren Sie Betroffene und Interessengruppen und involvieren Sie den Datenschutzbeauftragten und Betriebsrat früh; wenn notwendig, auch die Betroffenen)
3. Prüfen Sie ob die Verarbeitung notwendig ist.
4. Identifizieren Sie Risikoquellen (Motive, Ziele, Wahrscheinlichkeit des Eintreffens)
5. Schätzen Sie das Risiko ab (physischer, materieller oder immaterieller Schaden, die Schwere und Wahrscheinlichkeit des Eintretens)
6. Wählen und dokumentieren Sie ein angemessenes Schutzniveaus, inklusive aller technischen und organisatorischen Maßnahmen
7. Erstellen Sie einen DSFA-Report, mit allen oben aufgelisteten Informationen.

Nach einer durchgeführten DSFA, sollte man die getroffenen Maßnahmen auf Effektivität prüfen.

V. Wie sich Mitarbeiter verhalten sollen

Es ist wichtig die Mitarbeiter einzubinden. Doch was sollen Mitarbeiter genau tun? Grundsätzlich gilt, dass in der Vergangenheit gelebte Prozesse neu überdacht werden sollten. Was, wenn ein Mitarbeiter z. B. mit der Einführung von Software, dem Einholen von Einverständniserklärungen oder der Wahl eines bestimmten Accounts betraut ist und er das außerhalb seiner Abteilung bisher kaum mitteilen musste? Machen Sie klar, dass auch solche Dinge natürlich datenschutzrechtlich überprüft werden müssen und ggf. auch Auftragsverarbeitungsverträge geschlossen werden müssen und je nach Schutzbedarf auch eine Datenschutzfolgeabschätzung (im Vorfeld) stattfinden sollte.

Die Mitarbeiter sollten grundsätzlich den Datenschutzbeauftragten kontaktieren und gemeinsam entsprechende Evaluierungen durchführen.

Auch ist es sinnvoll alle darauf hinzuweisen, dass mögliche Datenskandale (wie Fremdzugriffe, Datendiebstahl etc.) ebenfalls unmittelbar gemeldet werden müssen. Hier könnte eine betriebliche Leitlinie helfen.

Des weiteren ist zu empfehlen, die Mitarbeiter regelmäßig zu schulen und auch auf andere Gefahren eines Datenleaks, wie Social Engineering, hinzuweisen bzw. darauf zu sensibilisieren. (Phising E-Mails, falsche Handwerker in der Firma, Anrufe etc.)

VI. Schlussgedanken

Die Regelungen in der DSGVO, sind teilweise noch unspezifisch. Hier sind Urteile von Gerichten bzw, weitere gesetzliche Änderungen wie die E-Privacy Verordnung oder die nationale Gesetzgebung zu beachten.

Sollten Sie privat Ihre Daten mit Facebook und Co. teilen, erlaubt Ihnen das nicht, mit den Daten anderer ebenfalls so umzugehen. Es sollte möglich sein, wie in der analogen Welt, seine Meinung, Gedanken und mögliche Geheimnisse zu teilen und sicher gehen zu können, dass diese vertraulich bleiben.

Heutzutage hat Big Data einen riesen (finanziellen und politischen) Wert und sollte keinesfalls unterschätzt werden:

- 2010 hatte Google einen Gewinn von 29,3 Mrd. US-$ [1] auf Grund von personalisierter Werbung (das war ist nur auf Grund der massiven Datensammlung überhaupt möglich und dieses Sammeln fand findet nicht nur auf Google-eigenen Seiten, sondern auch auf Seiten der Werbepartner (Adsense), auf dem Android Betriebssystem und Google Analytics zu).
- Big Data hatte ebenfalls einen massiven Einfluss auf die Wahlen von Obama[2] und Trump[3]. Ein Team von 100 Menschen analysierte Terabytes von Daten, um die Kampagnen zu optimieren.
- Einige Firmen nutzen Fitness-Tracker-Bonus-Programme. Wenn Sie sich gesund ernähren und Sport machen, bekommen Sie Rabatte auf Ihre Versicherung.

In der Vergangenheit haben die Menschen die Wichtigkeit des Schutzes ihrer Daten wenig Bedeutung zugemessen. Jedoch wurden “früher” auch die Daten nicht in diesem Umfang gesammelt, ausgewertet und zwischen so vielen Drittdienstleistern ausgetauscht.

---

[1]

[2]https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/

[3]https://www.cbc.ca/radio/day6/episode-359-harvey-weinstein-a-stock-market-for-sneakers-trump-s-data-mining-the-curious-incident-more-1.4348278/data-mining-firm-behind-trump-election-built-psychological-profiles-of-nearly-every-american-voter-1.4348283

Auf Grund der täglich wachsenden Internationalität der Datensammler, dem stetig wachsenden Datenberg, sowie der fehlenden internationalen (außer-europäischen) Strafverfolgung bei Vergehen, gibt es hier derzeit noch kein Allheilmittel.

Also denken Sie daran, wenn...

- Sie eine E-Mail weiterleiten...
- Sie personenbezogene Daten an andere Personen schicken...
- Sie Visitenkarten[1] drucken
- Sie personenbezogene Informationen per Telefon oder E-Mail herausgeben
- Sie Daten auf einem Formular abfragen, um Profile oder ähnliches anzulegen
- Sie personenbezogene Daten auf dem Smartphone speichern
- Sie personenbezogene Daten in ein Webformular kopieren/eingeben
- Sie personenbezogene Informationen generell weiterleiten
- Ihr Unternehmen bedenkliche Systeme[2] einführt d

Weiterführende Links finden Sie weiter unten oder auf unserer Website anoxinon.media.

Wenn Ihnen diese Präsentation gefallen hat oder Sie Verbesserungsvorschläge haben, schreiben Sie und doch eine E-mail: redaktion@anoxinon.de

Vielen Dank fürs Durchlesen!

Weiterführende Links:

www.edri.org - European Digital Rights (EDRi)

www.dlapiperdataprotection.com – Vergleich der weltweiten Datenschutzgesetzen

www.exodus-privacy.eu.org – Überprüfung von Apps auf Tracker o.ä.

www.privacytools.io – Empfehlungen für privatspähren freundliche Software

https://digitalcourage.de/digitale-selbstverteidigung/unternehmen-und-organisationen – Beitrag des Vereins Digitalcourage mit vielen Vorschläge über Alternativen

www.zdnet.de/88347263/niederlande-sammlung-von-microsoft-office-telemetriedaten-verstoesst-gegen-dsgvo – Beitrag über Verstoß von Microsoft Office gegen die DSGVO

[1] https://www.indigorise.de/dsgvo-abmahnfalle-visitenkarte/
[2] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html