DATENSCHUTZ G.A.S.

FAHRPLAN ZUR VORBEREITUNG AUF DIE DSGVO
Datenschutz, wie geht das?

ÜBERBLICK

WELCHE UNTERNEHMEN SIND BETROFFEN?

- Unternehmen mit Sitz in der EU, die Daten von Unionsbürgern verarbeiten
- Außereuropäische Unternehmen unterliegen der DSGVO, sobald sie eine Niederlassung in der EU besitzen oder Daten von Unionsbürgern verarbeiten.

Datenschutz geht alle an. Die DSGVO gilt daher sowohl im B2B- als auch im B2C-Bereich, online und stationär in allen Branchen.
Betroffene sollen vor jeder Verarbeitung ihrer Daten eine Zustimmung geben, wenn keine andere gesetzliche Erlaubnis vorliegt. Betroffene haben mehr Rechte (z. B. Auskunftsrechte, Beschwerderecht). Die Pflichten für Unternehmen erhöhen sich.
Unter die DSGVO fallen nur personenbezogene Daten, d. h. Daten, die auf einebestimmte, natürliche Person zurückzuführen sind. Anonyme Datenverarbeitung ist NICHT von der DSGVO erfasst.

ES SIND BUSSGELDER MÖGLICH IN HÖHE VON…

- bis zu 4 Prozent des gesamten weltweiten Jahresumsatzes eines Unternehmens bzw.
- 20 Millionen Euro

Die neue Europäische Datenschutzgrundverordnung (DSGVO) wird globale Ausmaße haben. Die Geltung beginnt am 25. MAI 2018 – sind Sie vorbereitet?
Was bedeutet die DSGVO für jeden Einzelnen?

ZIEL

- Schutz für persönliche Daten erhöhen
- Strafen für Datenschutzverstöße anheben
- Regulierungsmacht auch außerhalb der EU-Grenzen erhöhen

G.A.Service GmbH • Siezenheimer Straße 39 • 5020 Salzburg • ga-service.at
Benjamin Beier • +43 662 45 25 95 46 • datenschutz@ga-service.at

DIE 5 GEBOTE BEIM DATENSCHUTZ

Wie jedes Gesetz stellt auch die DSGVO Grundregeln auf, die sich durch die Vorschriften ziehen, wie ein roter Faden. Bei allen Datenvorgängen im Unternehmen müssen folgende Prinzipien angewandt werden:

1

VERBOT MIT ERLAUBNISVORBEHALT

Jede Datenverarbeitung, die nicht durch eine Einwilligung des Betroffenen abgedeckt ist, bedarf einer gesetzlichen Erlaubnis. Ansonsten dürfen die Daten nicht verarbeitet werden. Dieser Grundsatz wird Ihnen in diesem Leitfaden immer wieder begegnen.
Beispiel: Für das Versenden von Newslettern gibt es natürlich keine pauschale gesetzliche Erlaubnis. Die Einwilligung ist von jedem Newsletter-Empfänger vorab einzuholen.

2

DATENSPARSAMKEIT

Eine Datenverarbeitung muss dem Zweck angemessen und sachlich relevant sowie auf das notwendige Maß beschränkt sein. Beispiel: Bei einer Warenbestellung darf keine Telefonnummer erhoben werden, da sie für die Bestellabwicklung nicht notwendig ist. Es werden lediglich Name und Anschrift und ggf. die Bankdaten (z. B. bei Lastschrift) benötigt.

3

ZWECKBINDUNG

Die Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden.
Beispiel: Die erhobene Adresse bei der Bestellung darf nur für die Bestellabwicklung genutzt werden. Selbstredend darf sie nicht ohne Zustimmung an Dritte
(z. B. eine Auskunftei) weitergegeben werden.

4

DATENSICHERHEIT

Bei der Verarbeitung von Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Schutz von Daten zu gewährleisten. Beispiel: Wer mit sensiblen Mitarbeiter-, Firmen- und Kundendaten arbeitet, muss gewährleisten, dass keine unberechtigte Person Zugriff auf sie hat (z. B. durch Passwörter, Verschlüsselung).

5

TRANSPARENZ

Betroffene sollen wissen, dass und welche Daten in Bezug auf ihre Person erhoben wurden.
Beispiel: Wer Daten (im Hintergrund), d. h. ohne Wissen des Webseitenbesuchers, erhebt, muss mindestens in der Datenschutzerklärung transparent darüber aufklären.

Schon beim virtuellen Betreten einer Webseite werden reihenweise Daten der Besucher erhoben, gespeichert und weiterverarbeitet. Das geht natürlich nur im Rahmen des gültigen Datenschutzrechtes. Das wird sich speziell beim Umgang mit Vertrags- und Kundendaten durch die DSGVO auch nicht ändern.

DIE NEUE DATENSCHUTZERKLÄRUNG

- Kontaktformular
- Hinweis auf Weitergabe von Daten
- Cookies
- Webanalyse- und Tracking-Tools
- Newsletter-Versand
- Hinweis auf Recht zur Auskunft
- Berichtigung, Sperrung und Löschung von Daten
- Name und Kontaktdaten des für den Datenschutz Verantwortlichen
- Ggf. die Kontaktdaten des Datenschutzbeauftragten
- Die Zwecke der Datenverarbeitung
- Die Rechtsgrundlage für die Verarbeitung
- Die berechtigten Interessen, die damit verfolgt werden
- Ggf. die Empfänger der Daten
- Ggf. die Absicht des Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- Die Speicherdauer
- Das Auskunftsrecht
- Das Berichtigungs-, Löschungs- oder Einschränkungsrecht
- Das Widerspruchsrecht
- Das Recht auf Datenübertragbarkeit (Info: Das Recht auf Datenübertragung gibt Personen einen Anspruch, ihre Daten in einer Datei zu erhalten). Der Nutzer hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen".
- Das Recht, die Einwilligung jederzeit zu widerrufen
- Das Beschwerderecht bei einer Aufsichtsbehörde

Der Verantwortliche hat der betroffenen Person alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Jede betroffene Person hat ein Anrecht darauf, zu erfahren, zu welchen Zwecken die betreffenden persönlichen Daten (weiter-)verarbeitet werden. Wie lange diese Daten gespeichert und nach welcher Logik die Daten einer automatisierten Entscheidungsfindung verarbeitet werden. Wer die Empfänger der Daten sind und welche Folgen eine solche Verarbeitung haben kann.

DIE NEUEN AUSKUNFTS- UND BETROFFENENRECHTE

Neben den erläuterten Informationspflichten haben Betroffene daher auch Auskunftsrechte, die durch die DSGVO festgelegt bzw. erweitert wurden. Jeder Person muss ein Auskunftsrecht gewährt werden, welches problemlos wahrgenommen werden kann. Jede betroffene Person hat das Recht, eine Bestätigung darüber zu erhalten, ob und welche ihrer Daten verarbeitet werden. Ist dies der Fall, besteht ein Recht auf Auskunft:

- Welcher Zweck wird mit dieser Datenverarbeitung verfolgt (z. B. personalisierte Werbung)
- Welche Kategorien von Daten sind betroffen (z. B. ethnische Herkunft oder politische Meinung)
- Empfänger, gegenüber denen die Daten offengelegt worden sind oder noch offengelegt werden (z. B. Auskunftei bei Bonitätsprüfung)
- Geplante Speicherdauer
- Recht auf Berichtigung, Löschung oder Einschränkung der Datenverarbeitung

INFO
Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender, unrichtiger Daten oder die Vervollständigung dieser zu verlangen. Betroffene haben ein Recht, dass ihre Daten gelöscht werden. Eine Unkenntlichmachung kommt beispielsweise zum Tragen, wenn die Daten für den Zweck, für den sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind (z. B. Bestellhistorie älter als zwei Jahre).

DIE AUFTRAGSVERARBEITUNG

Bei der Auftragsverarbeitung erhebt, verarbeitet und/oder nutzt ein externer Dienstleister die personenbezogenen Daten für einen anderen „Auftraggeber". So stellen z. B. folgende Datenverarbeitungsprozesse eine Auftragsverarbeitung dar:

- Nutzung externer Serverkapazitäten
- Nutzung eines externen Callcenters
- Entsorgung von Datenträgern oder Akten
- Nutzung von Google Analytics

Der Auftraggeber, der die Daten seiner Webseitenbesucher oder andere persönliche Daten von anderen nutzen lässt, behält die volle Verantwortlichkeit, dass der Datenschutz nicht verletzt wird. Die Daten dürfen nur anhand der konkreten Weisungen des Auftraggebers genutzt werden. Der Auftraggeber weist und kontrolliert somit jeden Schritt der Datenverarbeitung und bleibt der Herr der Daten. Kommt es bei einem Auftragsverarbeiter zu einem Datenschutzverstoß, muss dieser seinen Auftraggeber informieren.

Der Auftraggeber darf nur mit solchen natürlichen oder juristischen Personen, Behörden, Einrichtungen oder anderen Stellen zusammenarbeiten, die hinreichend garantieren können, dass sie die Verarbeitung der Daten im Einklang mit dem Datenschutzrecht gewährleisten können. Weiterhin ist erforderlich: der Vertrag über die Auftragsverarbeitung inkl. Verschwiegenheitsklausel in elektronischer oder schriftlicher Form.

BEISPIEL

Ein Callcenter bekommt den Auftrag, für einen Auftraggeber eine Bestellannahme durchzuführen. Das Callcenter tritt nicht als eigenständiges Callcenter auf, sondern im Namen des Auftraggebers. Dem Callcenter ist es verboten, die übermittelten oder neu gesammelten Daten für weitere oder eigene Zwecke weiter zu nutzen. Denken Sie an Folgendes, wenn Sie Daten zur Auftragsverarbeitung weitergeben:

- Der Auftraggeber haftet für die Datenschutzverstöße des Auftragnehmers, wählen Sie Ihre Vertragspartner also sorgfältig aus.
- Der Auftraggeber weist und kontrolliert die externe Datenverarbeitung.
- Der Auftraggeber ist verpflichtet, die Weisungen zu dokumentieren.
- Der Auftraggeber ist verpflichtet, Sicherheitsvorfälle zu dokumentieren.
- Der Abschluss eines Auftragsverarbeitungsvertrages ist erforderlich.

ÄNDERUNGEN BEI COOKIES, WEBANALYSE-TOOLS UND SOCIAL PLUGINS

Das Internet kann in Sachen Tracking dank Cookies und Co. ein transparenteres Bild seiner Kunden nachzeichnen. Nicht nur die großen Unternehmen wie Amazon, Facebook oder Google arbeiten mit Cookies und Analyse-Tools, sondern auch auf kleineren Webseiten werden meist standardmäßig Cookies zur Analyse von Nutzerprofilen gesetzt. Viele Webseitenbetreiber sind sich aber gar nicht im Klaren, dass sie massenhaft persönliche Daten ihrer Webseitenbesucher abgreifen und an (unbekannte) Server übermitteln.

INFO
Ein Cookie-Banner (etwa über ein Pop-up) war bislang und wird auch künftig nicht notwendig sein. Nach den neuen Regeln gilt der erstmalige Besuch der Website ohnehin nicht als Einwilligung in die Verarbeitung von Besucherdaten, auch wenn Sie Ihren Besuchern Informationen wie "Durch die Nutzung dieser Webseite akzeptieren Sie Cookies" zur Verfügung stellen.

COOKIES

Checkliste für einen DSGVO-konformen Cookie

- Verständliche Klausel in der Datenschutzerklärung über Funktionsweise und Zweck der/des Cookie(s)
- Hinweis auf die Opt-out-Möglichkeit in den Browsereinstellungen, wahlweise mit Anleitung
- Allgemeine Informationspflichten zu Cookies (neu ist insbesondere die Rechtsgrundlage und der Zweck der Datenverarbeitung, s. o. zum Punkt „Informationspflichten")
- Respekt vor den „DoNotTrack"-Einstellungen

TRACKING- UND ANALYSE-TOOLS

Bei nicht selbst gehosteten Lösungen werden die persönlichen Daten der Webseiten-Besucher oft und für den Internetnutzer unbemerkt an externe Server übermittelt. Werden personenbezogene Daten, d. h. Daten, die Rückschluss auf eine bestimmte natürliche Person zulassen (z. B. IP-Adresse), der Webseitenbesucher abgegriffen, weitergeleitet und ausgewertet, ist weiterhin eine ausführliche Datenschutzerklärung mit Erklärungen über Funktionsweise, Rechtsgrundlage und Empfänger der Daten unerlässlich.

Eine explizite Einwilligung vom Besucher benötigt der Webseiten-Betreiber auch weiterhin nicht, da er ein berechtigtes Interesse daran hat, etwas über die Vorlieben der Kunden zu erfahren, um dadurch zielgerichtete Werbung schalten zu können. Da der Kunde auf sein jederzeitiges Widerspruchsrecht hingewiesen werden muss, sind seine Daten ausreichend geschützt.

SOCIAL PLUGINS

Seit es den Like-Button bei Facebook – und später weitere Plugins anderer Netzwerke – gibt, warnen Datenschützer vor ihnen. Warum? Weil das Netzwerk Daten der Internetnutzer abgreift, ohne zu informieren, welche das sind, wo sie letztendlich landen und was mit ihnen passiert.

Wie wir bereits gelernt haben, dürfen persönliche Daten nur verarbeitet werden, wenn der Betroffene vorher einwilligt oder eine andere Rechtsgrundlage vorliegt. Doch es gibt – wie so oft – ein „Aber". Der Einsatz von Plugins könnte auch künftig an ausreichenden Informationen scheitern. Wie bislang auch, muss der Betroffene informiert werden, in welche Datennutzung genau er einwilligt.

Vor seinem Mausklick muss also unter anderem bekanntgegeben werden, wer genau die Daten erhebt, speichert und nutzt und aus welchem Grund dies getan wird.
Da die sozialen Netzwerke nur in begrenztem Umfang Auskunft geben, welche Daten sie erheben und wohin diese gelangen, wird auch künftig kein sorgenloser Einsatz von Plugins möglich sein. Daher werden auch ab 2018 die Behelfsmöglichkeiten Shariff-Button oder 2-Klick-Lösung nicht verschwinden.

E-MAIL-WERBUNG

Wer einmal im Internet unterwegs ist, bekommt früher oder später virtuelle Post. Wie der Absender der E-Mails an die E-Mail-Adresse gekommen ist, bleibt dabei oft ein Rätsel.

Für die Empfänger kann die E-Mail-Flut jedoch eine echte Belästigung sein, weshalb der Gesetzgeber strenge Regelungen an die Versendung von E-Mail-Werbung aufgestellt hat. Aktuell gilt, dass die vorherige und ausdrückliche Einwilligung des Adressaten erforderlich ist, um diesem eine Werbe-E-Mail zusenden zu dürfen. Liegt die Einwilligung nicht vor, stellt dies eine unzulässige Belästigung des Empfängers dar.
Der Versender ist für das Vorliegen dieser Einwilligung des Adressaten beweispflichtig.
Die für die Praxis überwiegend empfohlene Variante ist daher das Double-Opt-in-Verfahren. Obwohl Newsletter in der Praxis höchste Relevanz haben, findet sich in der DSGVO selbst keine explizite Regelung für deren Versendung. Herhalten müssen daher – wie eingangs erwähnt – die allgemeinen Prinzipien. Relevant ist hier das sogenannte „Verbot mit Erlaubnisvorbehalt“:

Die Nutzung einer E-Mail-Adresse für Newsletter und E-Mail-Werbung ist nur zulässig, wenn:
- die Einwilligung des Empfängers oder
- ein sogenanntes „berechtigtes Interesse“ vorliegt.

HINWEIS

Für das Versenden von Newslettern gibt es keine pauschale gesetzliche Erlaubnis. Die Einwilligung ist von jedem Newsletter-Empfänger gesondert und vorab einzuholen.

1

VARIANTE 1:
VERSENDUNG MIT VORHERIGER EINWILLIGUNG

Die Einwilligung muss auch mit der DSGVO durch eine ausdrückliche Handlung des Adressaten (bewusst und eindeutig) und nur für einen konkreten Fall erfolgen. Wegen der Nachweispflicht sollte auch weiterhin am Double-Opt-in-Verfahren festgehalten werden.

2

VARIANTE 2:
VERSENDUNG AUFGRUND EINES BERECHTIGTEN INTERESSES (DIREKTWERBUNG)

Neben der DSGVO ist auch die E-Privacy-Richtlinie zu beachten, die ein Verbot unaufgeforderter E-Mail-Werbung vorsieht. Dies schlägt sich auch im österreichischen Recht (§107 TKG) nieder, wo die Zusendung belästigender Werbung verboten ist. Auch die kommende E-Privacy-Verordnung – die die DSGVO in vielen Teilen ab 2019 ergänzen soll – sieht in ihrem aktuellen Entwurf ein Verbot von unaufgeforderter Werbung vor. Damit geht der sicherste Weg der E-Mail-Werbung auch weiterhin nur über die vorherige Einwilligung.

UMGANG MIT DATENPANNEN

Kommt es tatsächlich zu einem unberechtigten Datentransfer oder einem vergleichbaren Vorfall, meldet der Verantwortliche dies unverzüglich und möglichst binnen 72 Stunden nach Kenntniserlangung der zuständigen Aufsichtsbehörde. Die DSGVO knüpft auch an die Risiken an, die für die Betroffenen entstehen können, beispielsweise immaterielle Schäden (z. B. Rufschädigung) oder finanzielle Verluste. Anders als jetzt gilt die Meldepflicht jedoch nicht nur bei Datenpannen mit besonders sensiblen Daten, sondern grundsätzlich für alle personenbezogenen Daten. Eine Meldepflicht gilt also dann nicht, wenn keine Risiken für die Betroffenen zu erwarten sind.

Unter einer Datenschutzverletzung versteht die DSGVO einen Vorfall, der zu einer unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten geführt hat.

DER DATENSCHUTZBEAUFTRAGTE IM UNTERNEHMEN

Compliance spielt besonders im Datenschutz eine wichtige Rolle, denn Unternehmen hantieren tagtäglich mit Datenmengen, darunter hochsensible Kundendaten wie Anschriften, Bankdaten oder Informationen zu den gekauften Produkten. Geraten sie in die falschen Hände, etwa von unautorisierten Mitarbeitern oder Dritten (z. B. Hackern), kann das ein ungeahntes Ausmaß haben. Um neben der behördlichen Überwachung von Datenvorgängen ein weiteres Kontrollinstrument zu haben, besteht für einige Unternehmen die Pflicht, einen Datenschutzbeauftragten zu bestellen.

Unternehmen werden zur Bestellung eines Datenschutzbeauftragten verpflichtet, wenn deren Kerntätigkeit (d. h. deren Hauptgeschäftsfeld) in einer Datenverarbeitung besteht und aufgrund ihres Zwecks oder ihres Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich ist.

AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN

- Unterrichtung und Beratung des Unternehmens in Datenschutzfragen
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften
- Schulungen und Zusammenarbeit mit Behörden

CHARAKTERISTISCH

- Weisungsfreiheit
- Zur Geheimhaltung verpflichtet

PRAXISTIPP
Unternehmen sollten sich überlegen, ob sie formell verpflichtet sind, einen Datenschutzbeauftragten zu benennen.

Datenschutzbeauftragte müssen der zuständigen Datenschutzbehörde gemeldet werden!

STRENGE AUFSICHT UND EFFEKTIVE RECHTSDURCHSETZUNG

Auch wenn Datenschutzverstöße in aller Munde sind. Beim Lesen der Pressemeldungen bekommt der Internet-User den Eindruck, dass nur die ganz Großen durch Sanktionen zur Raison gerufen werden. Die DSGVO bekennt sich aber nun zu mehr Datenschutz – und den will sie auch durchfechten. In puncto Datenschutz heißt das, unabhängige und handlungsfähige Aufsichtsbehörden einzurichten und mit den technischen, personellen und finanziellen Mitteln auszustatten.

JEDE AUFSICHTSBEHÖRDE DARF UNTER ANDEREM

- Datenschutzüberprüfungen durchführen
- auf einen vermeintlichen Verstoß gegen die DSGVO hinweisen
- Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, verlangen
- Verantwortliche in Datenschutzfragen beraten

DIE AUFSICHTSBEHÖRDE KANN UNTER ANDEREM

- verwarnen, wenn bereits ein Verstoß gegen die DSGVO vorliegt
- anweisen, Betroffenen Auskünfte zu erteilen oder Betroffenenrechte durchzusetzen
- anweisen, Datenverarbeitungsvorgänge wieder in Einklang mit der DSGVO zu bringen
- anweisen, den/die Betroffenen bei Datenschutzverstößen zu informieren
- Beschränkungen oder Verbote einer Datenverarbeitung verhängen
- Geldbußen verhängen
- die Übermittlung von Daten an Drittstaaten stoppen

Hierfür stehen den Datenschutzbehörden künftig umfangreichere Befugnisse zur Seite. Zudem werden die Sanktionsmöglichkeiten ausgedehnt.

Unternehmen: Auch diese müssen nur noch mit der für sie zuständigen Datenschutzbehörde zusammenarbeiten, also mit der des Mitgliedstaates, in dem sich ihr Hauptsitz befindet.

VERARBEITUNGSVERZEICHNIS, VORABKONTROLLE UND FOLGENABSCHÄTZUNG

Um mit der DSGVO überhaupt beginnen zu können, müssen sich zunächst alle betroffenen Unternehmen einen Überblick verschaffen, welche Daten sie überhaupt in ihrem Unternehmen verarbeiten. Hier kommt oft Ungeahntes zutage, denn sowohl mit Mitarbeiter- als auch mit Kundendaten kommt eine große Summe zusammen, deren sich die Verantwortlichen meist gar nicht bewusst sind. Nur mit einem Sachstand über alle Datenvorgänge können die neuen Vorschriften der DSGVO angewandt werden.

Sichten Sie daher zunächst einmal, welche Daten Sie in Ihrem Unternehmen verarbeiten, um dann mit der eigentlichen Umsetzung der DSGVO beginnen zu können. Dies dient im Übrigen nicht nur dazu, sich einen generellen Sachstand über alle Datenprozesse im Unternehmen zu verschaffen. Für Unternehmen besteht mit der DSGVO sogar die Pflicht, ein sogenanntes „Verarbeitungsverzeichnis" zu führen, welche die Datenverarbeitungsprozesse
im Unternehmen katalogisiert.

PFLICHT ZUR ERSTELLUNG EINES VERARBEITUNGSVERZEICHNISSES

Die Pflicht zur Führung eines Verarbeitungsverzeichnisses gilt nach der DSGVO grundsätzlich für alle Unternehmen, welche personenbezogene Daten verarbeiten. Ausnahmen sind streng reguliert. Zum anderen haben Unternehmen Informations- und Auskunftspflichten auch gegenüber den Betroffenen, beispielsweise gegenüber den Kunden, mit deren Daten gearbeitet wird. Mit einem aufbereiteten Verarbeitungsverzeichnis können die Unternehmen den Anfragen leichter Herr werden und sich gut auf die neuen Anforderungen der DSGVO vorbereiten.

INHALT EINES VERARBEITUNGSVERZEICHNISSES

Unternehmen arbeiten massenhaft mit persönlichen Daten. Im Online-Handel ist das vornehmlich die Kundendatei mit sensiblen Anschriftsdaten oder Zahlungsinformationen (z. B. Kreditkartendaten). Sind Angestellte im Unternehmen vorhanden, kommen auch deren persönliche Daten hinzu. Für Unternehmen besteht daher die Pflicht, ein Verarbeitungsverzeichnis zu führen, welches die Datenverarbeitungsprozesse im Unternehmen katalogisiert. Dieses Verarbeitungsverzeichnis enthält u. a. die folgenden Angaben:

- Name und Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Empfänger, gegenüber denen die Daten offengelegt worden sind oder noch offengelegt werden

GEHEN SIE FOLGENDE PROZESSE IN BEZUG AUF IHREN DATENBEZUG DURCH:

- Verarbeitung der Daten von Kunden (Vertragsdaten, Kontaktdaten, Kaufhistorie, Zahlungsdaten, Bonitätsprüfung usw.)
- Analyse- und Tracking-Tools
- Cookies
- Social Plugins
- Welche Datenverarbeitungsprozesse werden an externe Stellen abgegeben
- Newsletter-Versand
- Steuerrechtliche Daten und Finanzmanagement (z. B. Lohnabrechnungen, Rechnungslegung bei Kunden und Lieferanten)
- Personalmanagement (z. B. Arbeitsverträge, Arbeitszeiterfassung, Bankverbindungen, Bewerbungsmanagement)
- Einkauf und Vertrieb (z. B. Lieferantenkontakte)
- Übersicht über externe Dienstleister
- Buchhaltung

Mittlerweile haben sich sogar professionelle Software-Anbieter an dem Thema versucht und Software zur Unterstützung beim Verfahrensverzeichnis auf den Markt gebracht. Aber auch die Datenschutzbehörden geben Muster heraus.

FOLGEN BEI VERSTÖSSEN

Die nationalen Behörden können zur Prüfung der Einhaltung des Datenschutzes Einsicht in das Verzeichnis verlangen und bei einem Versäumnis Bußgelder verhängen. Wird das Verarbeitungsverzeichnis nicht geführt oder ist lückenhaft, können dem Verantwortlichen Geldbußen von bis zu 10 Millionen Euro oder von bis zu 2 Prozent des weltweit erzielten Jahresumsatzes aus dem vergangenen Geschäftsjahr auferlegt werden.

DIE VORABKONTROLLE UND DIE FOLGENABSCHÄTZUNG

Nach der DSGVO muss der Verantwortliche künftig nur dann vorab seine Verarbeitungsprozesse behördlich überprüfen lassen, wenn die sogenannte Folgenabschätzung („Data Protection Impact Assessment") ergibt, dass ein hohes Risiko für die Daten besteht (z. B. beim Profiling) und keine anderweitigen Vorkehrungsmaßnahmen getroffen wurden. Mit der DSGVO ist daher zunächst eine Folgenabschätzung durchzuführen. Birgt die Datenverarbeitung voraussichtlich ein hohes Risiko für die Betroffenen, muss der Verantwortliche bereits vor Einführung eines neuen Datenverarbeitungsprozesses eine Abschätzung der Folgen durchführen (sogenannte Folgenabschätzung). Dies ist insbesondere bei neuen Technologien der Fall, bei denen Umfang und Eingriff in die Persönlichkeitsrechte noch nicht feststehen. Die DSGVO nennt bestimmte Fallgruppen, bei denen eine Folgenabschätzung stets durchzuführen ist. Dazu zählen:

- Profiling
- Verarbeitung besonders sensibler Daten (z. B. Gesundheitsdaten)
- Einsatz neuer Technologien
- Umfangreiche, öffentliche Videoüberwachung

GLOSSAR

AUFSICHTSBEHÖRDE(N)
ist/sind die vom jeweiligen Mitgliedstaat eingerichtete(n) Behörde(n), die der unabhängigen Datenschutzaufsicht dient/dienen und die Einhaltung der DSGVO überwachen soll(en).

AUFTRAGSVERARBEITER
ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (siehe auch „Verarbeitung").

AUFTRAGSVERARBEITUNG
ist die Verarbeitung (siehe auch „Datenverarbeitung") personenbezogener Daten durch externe Dienstleister für den Auftraggeber.

BETROFFENER
ist die Person, deren persönliche Daten berührt werden.

CODE OF CONDUCT
sind Verhaltensregeln für den Umgang mit personenbezogenen Daten, die von den Aufsichtsbehörden genehmigt werden, insbesondere Anleitungen, wie der Verantwortliche oder Auftragsverarbeiter die Datenverarbeitung durchzuführen hat und wie die Einhaltung der Anforderungen nachzuweisen ist.

DATENSICHERHEIT
bedeutet, dass der Verantwortliche unter Berücksichtigung des Stands der Technik oder des Zweckes der Datenverarbeitung geeignete Maßnahmen umzusetzen hat, um die Sicherheit der Daten zu gewährleisten (z. B. Verschlüsselung, Passwörter).

DATENMINIMIERUNG
bedeutet, dass die Datenverarbeitung auf das notwendige Maß beschränkt sein muss, beispielsweise dürfen bei einer Anfrage nur die Kontaktdaten der Person und das Geburtsdatum abgefragt werden.

FAHRPLAN ZUR VORBEREITUNG AUF DIE DSGVO

1. Sensibilisierung und interne Datenschutzorganisation
2. Bestimmung eines Datenschutzbeauftragten bzw. -verantwortlichen bestimmen
3. Dateninventur durchführen (Verarbeitungsverzeichnis)
4. Vertrautmachen mit neuen Auskunfts- und Betroffenenrechten
5. Verträge zur Auftragsverarbeitung anpassen
6. Zustimmungen und Einwilligungen überprüfen
7. Shop bzw. Webseite datenschutz-konform gestalten
8. Newsletter-Versand anpassen
9. Neue Datenschutzerklärung organisieren
10. Rechtliche Entwicklungen beobachten

QUELLE

Leitfaden zur Vorbereitung auf die Datenschutzgrundverordnung (DSGVO), verfasst von Yvonne Bachmann, Händlerbund, Stand März 2018.