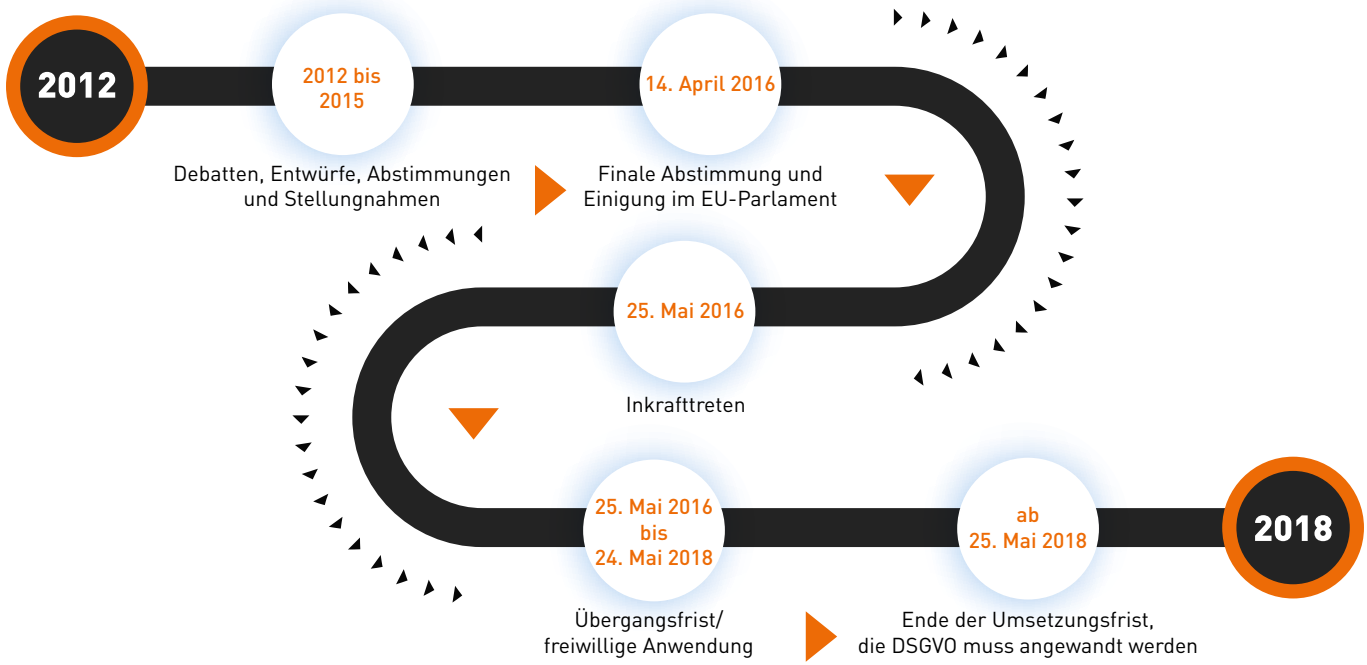
Stand: März 2018

„HOW TO“ LEITFADEN

zur Vorbereitung auf die Datenschutzgrundverordnung (DSGVO)

Verfasst von Yvonne Bachmann,
Rechtsanwältin des Händlerbund

HÄNDLERBUND



EINLEITUNG

Eine Chance für die Stärkung des Datenschutzes oder ein bürokratisches Monster? Die Meinungen zu einem Thema gingen selten so weit auseinander wie bei der neuen Datenschutzgrundverordnung (nachfolgend: DSGVO). Kein Wunder, dass die DSGVO so viele Jahre auf sich warten ließ. Ein langer und steiniger Weg liegt hinter den neuen Vorschriften, denn schließlich mussten die Interessen von 28 Mitgliedstaaten unter einen Hut gebracht werden.

Vorgänger und Basis des derzeitigen Datenschutzes in der EU ist eine Richtlinie aus dem Jahr 1995. Damals gab es noch keine Smartphones oder Tablets. Selbst unter Google konnte sich noch kein Mensch etwas vorstellen, denn die Suchmaschine ging erst Jahre später an den Start. Kein Wunder, dass es in den darauffolgenden Jahren Datenskandale wie am Fließband gab, denn bei der rasanten technischen Entwicklung kamen weder Gesetze noch Gerichte hinterher.

Eine einheitliche, im gesamten EU-Raum geltende Datenschutzgrundverordnung soll damit nun endlich Schluss und reinen Tisch machen. Die neuen Vorschriften haben nicht nur zum Ziel, den Menschen mehr Kontrolle über ihre persönlichen Daten zu geben. Auch Behörden und Unternehmen sollen sich auf ein europaweit einheitliches Recht stützen, auf das sie vertrauen können.

Doch diskutiert und verhandelt wurde zur DSGVO erst einmal genug. Es ist Zeit, dass die Ärmel hochgekrempelt werden und tatsächlich Taten folgen. Mit diesem Leitfaden wird es Händlern sofort und ohne große Schwierigkeiten möglich sein, mit den Vorbereitungen auf die DSGVO zu starten, um sich alsbald wieder auf ihr eigentliches Geschäftsfeld, den Handel, konzentrieren zu können.

Ich wünsche Ihnen ein gutes Gelingen bei der Umsetzung der rechtlichen Vorschriften und weiterhin viel Erfolg bei Ihrem Online-Geschäft.

Ihr Andreas Arlt
Bundesvorsitzender des Händlerbundes

INHALTS-VERZEICHNIS

EINLEITUNG 02

1 / ÜBERBLICK 04

2 / NEUERUNGEN BEIM UMGANG MIT KUNDENDATEN 05

3 / DIE NEUE DATEN-SCHUTZERKLÄRUNG 06

4 / DIE NEUEN AUS-KUNFTS- UND BETROFFENENRECHTE 08

5 / DIE AUFTRAGS-VERARBEITUNG 09

6 / ÄNDERUNGEN BEI COOKIES, WEBANALYSE-TOOLS UND SOCIAL PLUGINS 10

7 / E-MAIL-WERBUNG 12

8 / UMGANG MIT DATENPANNEN 13

9 / DER DATENSCHUTZ-BEAUFTRAGTE IM UNTERNEHMEN 14

10 / STRENGE AUFSICHT UND EFFEKTIVE RECHTS-DURCHSETZUNG 15

11 / VERFAHRENSVERZEICHNIS, VORABKONTROLLE UND FOLGENABSCHÄTZUNG 23

GLOSSAR 20

FAHRPLAN ZUR VORBE-REITUNG AUF DIE DSGVO 23

1 / ÜBERBLICK

WER IST 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.

Unter die DSGVO fallen nur personenbezogene Daten, d. h. Daten, die auf eine bestimmte, natürliche Person zurückzuführen sind. Anonyme Datenverarbeitung ist NICHT von der DSGVO erfasst.

ES SIND BUß-GELDER MÖGLICH IN HÖHE VON...

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

88 SEITEN LANG

99 ARTIKEL

DER OFFIZIELLE TITEL LAUTET:
„Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG".

DER ERSTE ENTWURF TAUCHTE 2011 AUF.

DIE DSGVO GILT VERBINDLICH AB DEM 25. MAI 2018.

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?

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.

ZIEL

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

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:

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.

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. Interessant für den Händler sind lediglich Name und Anschrift und ggf. die Bankdaten (z. B. bei Lastschrift).

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.

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).

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.

2 / NEUERUNGEN BEIM UMGANG MIT KUNDENDATEN

Online-Handel ohne Datenverarbeitung? Undenkbar! 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.

Nach der DSGVO ist eine „echte“ Anfrage der betroffenen Person Pflicht, um deren Daten überhaupt verarbeiten zu dürfen. Alle Vertragsdaten, die der Webseitenbetreiber erhalten hat und die für die inhaltliche Ausgestaltung oder Änderung eines Vertrages erforderlich sind (Bestandsdaten), dürfen auch weiterhin verwendet werden – ohne gesonderte Einwilligung des Kunden. Gleiches gilt für die Nutzungsdaten (z. B. Zugangsdaten), deren Verarbeitung durch die DSGVO legitimiert ist.

3 / DIE NEUE DATENSCHUTZ-ERKLÄRUNG

Ohne die Erhebung und Speicherung von personenbezogenen Daten funktioniert der Online-Handel nicht. Warum? Natürlich müssen Kunden, um eine Bestellung aufgeben zu können, auch persönliche Daten eingeben (z. B. Name, Anschrift, E-Mail-Adresse). Im Online-Handel wird jedoch auch eine Vielzahl von weiteren Daten erhoben. So werten Tracking- und Analyse-Tools massenhaft Daten aus, die einer bestimmten Person zuordenbar sind.

Hier geht es dem Datenschutz besonders um die Aufklärung und Transparenz, denn der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ist ein europäisches Grundrecht. Jeder Webseitenbetreiber, der personenbezogene Daten erhebt und verarbeitet, muss deshalb eine Datenschutzerklärung verwenden. Zu informieren ist in der Datenschutzerklärung über Folgendes:

- dass Daten gespeichert werden
- Art, Umfang und Zwecke der Erhebung, Verarbeitung oder Nutzung/Verwendung personenbezogener Daten.

Klingt ziemlich abstrakt. Webseitenbetreiber können für die praktische Umsetzung folgende Checkliste verwenden. Fragen Sie sich ganz kritisch, ob folgende Punkte auf Sie zutreffen und prüfen, ob Ihre Datenschutzerklärung schon eine Klausel dazu enthält:

DATENVERARBEITUNG		
KONTAKTFORMULAR		
KOMMENTARFUNKTIONEN UND KUNDENBEWERTUNGEN		
HINWEIS AUF WEITERGABE VON DATEN		
COOKIES		
WEBANALYSE- UND TRACKING-TOOLS		
SOCIAL-PLUG-INS		
GOOGLE REMARKETING ODER ADWORDS CONVERSION TRACKING, O. Ä.		
NEWSLETTER-VERSAND		
ZAHLARTEN MIT BONITÄTSPRÜFUNG		
HINWEIS AUF RECHT ZUR AUSKUNFT,		
BERICHTIGUNG, SPERRUNG UND LÖSCHUNG VON DATEN		

Doch damit noch nicht genug ... Die Datenschutzerklärung erhält spätestens ab dem 25. Mai 2018 jedoch noch neue Klauseln:

Informationspflichten, wenn Daten direkt von der Person erhoben werden, z. B. beim Einsatz von Analyse-Tools, im Registrierungsvorgang	**Informationspflichten, wenn die Daten nicht von der Person direkt erhoben wurden,** z. B. bei Nutzung öffentlicher Quellen
► Namen 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 (z. B. bei US-amerikanischen Analyse-Tools); ► 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“ (z. B. Stromanbieterwechsel). ► das Recht, die Einwilligung jederzeit zu widerrufen; ► das Beschwerderecht bei einer Aufsichtsbehörde;	
► ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist; ► ob die Person verpflichtet ist, die Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte; ► Änderung des Zwecks der Datenverarbeitung.	► die Kategorien von Daten, die verarbeitet werden; ► aus welcher Quelle die Daten stammen und gegebenen falls ob sie aus öffentlich zugänglichen Quellen stammen.

Der Clou: Der Verantwortliche hat der betroffenen Person alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Hier entsteht ein Spannungsfeld zwischen hoch komplizierten technischen Abläufen (z. B. bei Cookies) und einer transparenten Informationserteilung.

Praxistipp: Die Erteilung der (alten und) neuen Informationspflichten ist für Online-Händler ohne juristische Hilfe schlicht und ergreifend nicht möglich. Die Reihe der Informationspflichten ist schier unüberschaubar und für den Laien nicht rechtssicher formulierbar. Bis Mai 2018 sollten sich Händler daher einen fachkundigen Beistand suchen, der ihnen bei der Umsetzung hilft und ihre Datenschutzerklärung auf das neue Recht anpasst.

Händlerbund-Mitglieder bekommen selbstverständlich automatisch und rechtzeitig ihre geänderten Rechtstexte zur Verfügung gestellt.

4 / DIE NEUEN AUSKUNFTS- UND BETROFFENENRECHTE

Jede betroffene Person hat ein Anrecht darauf, zu wissen und zu erfahren, zu welchen Zwecken sie betreffende, persönliche Daten (weiter)verarbeitet werden, wie lange diese gespeichert werden, wer die Empfänger der Daten sind, nach welcher Logik die Daten einer automatisierten Entscheidungsfindung verarbeitet werden und welche Folgen eine solche Verarbeitung haben kann.

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 ihre persönlichen Daten verarbeitet werden. Ist dies der Fall, besteht ein Recht auf Auskunft:
welche Daten betroffen sind;

- ✓ welcher Zweck mit dieser Datenverarbeitung verfolgt wird (z. B. personalisierte Werbung);
- ✓ welche Kategorien von Daten betroffen sind (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 unvollständiger Daten 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).

- ✓ Widerspruchsrecht gegen die (weitere) Datenverarbeitung;
- ✓ Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde;
- ✓ die Herkunft der Daten, wenn sie nicht bei der betroffenen Person erhoben werden;
- ✓ werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien unterrichtet zu werden.

Kommt ein Betroffener mit einer oder mehreren der genannten Auskunftsersuchen auf das Unternehmen zu, so ist die Auskunft:

- unentgeltlich
- unverzüglich (spätestens innerhalb eines Monats)

zu erteilen.

Auch mit dem „Recht auf Vergessenwerden“ als Spezialform des Löschungsanspruchs können sich Unternehmen künftig konfrontiert sehen. Wie funktioniert das Recht auf Vergessenwerden in

der Praxis? Die betroffene Person muss die datenverarbeitende Stelle (z. B. soziales Netzwerk) informieren, dass sie die Löschung aller Daten/Kopien von Daten und Links zu diesen Daten verlangt.

Praxistipp: Jeder Online-Händler, der schon einmal mit solchen Auskunftsverlangen zu tun hatte, wird wissen, wie unverhofft die Aufforderungen kommen können. Meist ist der Laie völlig überfordert, ob und welche Daten überhaupt herauszugeben sind.

Nutzen Betroffene ihre neu hinzugewonnen Rechte, dann sollte jedes Unternehmen zumindest ein Stück weit darauf vorbereitet sein.

5 / DIE AUFTRAGSVERARBEITUNG

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

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

Auftragsverarbeitung = Verarbeitung von Daten im **Auftrag** für einen anderen.

Der Online-Händler, 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 Online-Händler eine Bestellannahme durchzuführen. Das Callcenter tritt nicht als eigenständiges Callcenter auf, sondern im Namen des Händlers. 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.

© Alexandra Ignatyeva/Shutterstock.com

6 / ÄNDERUNGEN BEI COOKIES, WEBANALYSE-TOOLS UND SOCIAL PLUGINS

Der Online-Handel 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 kleinere Webseiten werden meist standardmäßig Cookies zur Analyse von Nutzerprofilen gesetzt. Viele Händler sind sich aber gar nicht im Klaren, dass sie massenhaft persönliche Daten ihrer Webseitenbesucher abgreifen und an (unbekannte) Server übermitteln.

Fragen Sie sich, ob die bevorstehende DSGVO-Gesetzgebung Auswirkungen auf die Art und Weise haben wird, wie Sie Ihre Webanalyse-Daten sammeln? Webanalyse ist heutzutage eines der wichtigsten Werkzeuge für Marketing und Business. Selbst bewährte Tools wie Matomo (ehemals Piwik) und Google Analytics bieten Ihnen bei einem unbedachten Einsatz keine Rechtssicherheit.

a) Cookies

Über die jahrelangen Diskussionen zur DSGVO hat man bestimmte technische Errungenschaften des modernen E-Commerce übersehen, die mittlerweile zum Standard im E-Commerce gehören. Weder Cookies noch Analyse-Tools finden ausdrückliche Erwähnung im DSGVO-Text – ob bewusst oder unbewusst, ist ein Rätsel.

Regelungen zu Cookies finden sich bisher in der ePrivacy-Richtlinie. Diese bleibt neben der DSGVO bestehen. Für die Vorbereitung auf den 25. Mai 2018 bedeutet das jedoch ein Vakuum, in welchem sich Juristen und Datenschützer trefflich über die Zukunft von Cookies streiten.

Die DSGVO regelt ausdrücklich die weitere Anwendbarkeit der ePrivacy-Richtlinie. Mithin bleiben auch die bisherigen Regelungen zu Cookies bestehen. Cookies können daher weiter gesetzt werden, wobei der Nutzer die Möglichkeit zum Widerspruch haben muss. (Opt-out).

Wie bislang auch, muss der Betroffene natürlich informiert werden, was mit seinen Daten geschieht. Es muss daher in der Datenschutzerklärung genau bekannt gegeben werden, wer genau die Daten erhebt, speichert und nutzt, aus welchem Grund dies getan wird und dass der Internetuser ein Widerspruchsrecht hat (siehe dazu auch die Informationspflichten).

Info: Ein Cookie-Banner (etwa über ein Popup) 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 Website akzeptieren Sie Cookies“ zur Verfügung stellen.

Weitergehende Aufklärung über die Voraussetzungen beim Cookie-Einsatz auf Webseiten wird erst die 2019 erwartete E-Privacy-Verordnung bringen.

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 Rechtsgrundage und der Zweck der Datenverarbeitung, s.o. zum Punkt „Informationspflichten“)
- ☐ Respekt vor den „DoNotTrack“-Einstellungen

b) 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 ein jederzeitiges Widerrspruchsrecht hingewiesen werden muss, sind seine Daten ausreichend geschützt.

Checkliste für DSGVO-konforme Webseiten-Analyse:

- ✓ Klausel in der Datenschutzerklärung für jedes Tool gesondert mit Ausführungen über Funktionsweise der Tools
- ✓ allgemeine Informationspflichten zu Cookies und Analyse-Tools (neu ist insbesondere die Rechtsgrundlage und der Zweck der Datenverarbeitung, s.o. zum Punkt Informationspflichten)
- ✓ Automatische Anonymisierung der Besucher-ID, insbesondere bei Google Analytics
- ✓ Respekt vor den „DoNotTrack“-Einstellungen
- ✓ Opt-out-Widget

c) Social PlugIns

Seit es den Like-Button bei Facebook – und später andere 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 von Internet-Surfern nur verarbeitet werden, wenn der Betroffene darin 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 bekannt gegeben 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.

7 / 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. Und in der Tat: „Nur jeder zehnte Online-Händler mailt rechtssicher", zeigt eine Studie der Unternehmensberatung Absolit Dr. Schwarz Consulting aus dem vergangenen Jahr.

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 sog. „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 sog. „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.

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.

Info: Schon vor Geltung der DSGVO ordnungsgemäß eingeholte Einwilligungen für den Erhalt von Newslettern bleiben bestehen. Dies haben die deutschen Aufsichtsbehörden festgelegt. Wer sich bisher an das Datenschutzrecht gehalten hat, kann mit den Einwilligungen also weiterarbeiten. Dennoch sollten die Einwilligungsprozesse auf die neuen Grundsätze der DSGVO hin geprüft und bei Bedarf angepasst werden.

Die Zusendung einer reinen Bestellbestätigung ist hingegen **gesetzlich gefordert** und damit keine E-Mail-Werbung und ohne Einwilligung erlaubt.

Exkurs: Mit der Freiwilligkeit einher geht auch das Koppelungsverbot. Beispielhaft zu nennen ist die Teilnahme an einem Gewinnspiel, welche an das Abonnement eines Newsletters gekoppelt ist. Hier wird es jedoch insbesondere bei Gratisangeboten noch Diskussionsbedarf geben, z. B. Download eines kostenfreien E-Books gegen Newsletter-Anmeldung. Das Bayerische Landesamt für Datenschutzaufsicht hierzu: „Daraus dürfte folgen, dass bei „kostenlosen" Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen" (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung"), diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar dargestellt werden muss. Raum oder Notwendigkeit für eine Einwilligung besteht dann nicht mehr."

Variante 2: Versendung aufgrund eines berechtigten Interesses (Direktwerbung)

Die Versendung von E-Mail-Werbung mit ausdrücklicher Einwilligung stellt den Regelfall dar. Nur ausnahmsweise ist die vorherige, ausdrücklich erteilte Einwilligung des Adressaten für den Erhalt eines Newsletters entbehrlich. Die Voraussetzungen sind jedoch sehr streng und in der Praxis derzeit kaum realisierbar. Die DSGVO selbst scheint deutlich offener: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Aber(!): Neben der DSGVO ist auch die E-Privacy-Richtlinie zu beachten, die ein Verbot unaufgeforderter E-Mail-Werbung vorsieht. Dies schlägt sich auch im deutschen Recht 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.

CHECKLISTE FÜR DIE VERSENDUNG VON E-MAIL-WERBUNG

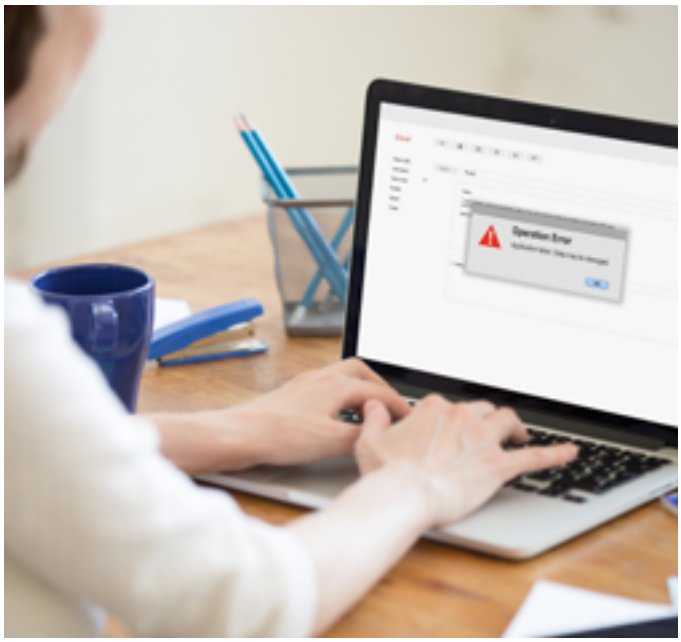
☐	Die Einwilligung muss durch eine ausdrückliche Handlung des Adressaten (bewusst und eindeutig, ohne vorausgewählte Häkchen, sog. Opt-out) erfolgen. Es bleibt das bisher übliche Double-Opt-in-Verfahren empfehlenswert.
☐	Das in der DSGVO hervorgehobene Kriterium der Freiwilligkeit der Einwilligung besagt, dass eine Einwilligung aus eigenem Antrieb und ohne jeden Zwang abgegeben werden muss. Die Einwilligung gilt nicht als freiwillig erteilt, wenn die Erfüllung eines Vertrags (z. B. die Bestellaufgabe und Warenlieferung) von der Einwilligung in den Newsletter abhängig ist.
☐	Es ist eine genaue Information (= Klausel in der Datenschutzerklärung) erforderlich, worin der E-Mail-Empfänger einwilligt (z. B. genaue Angaben zum Absender des Newsletters, zum Intervall des Newsletters, zum Inhalt der Newsletter, z. B. „Neues im Shop“).
☐	Der für den Newsletter-Versand Verantwortliche muss die Einwilligung belegen können.
☐	Die betroffene Person hat auch weiterhin das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Adressat muss auf diese Abbestellmöglichkeit hingewiesen werden, und zwar sowohl beim Bestellen des Newsletters als auch in jedem Newsletter durch Abbestellmöglichkeit sowie in der Datenschutzerklärung auf der Webseite. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

8 / UMGANG MIT DATENPANNEN

Zahlreiche Datenpannen, die von den Unternehmen bagatellisiert und von Behörden ignoriert wurden, waren einer der Anlässe für ein neues Daten„schutz“recht in Europa. Die DSGVO schafft daher ausdrücklich eine verschärfte Pflicht zur Meldung von Datenschutzverletzungen an die Behörden.

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.



© fizkes/Shutterstock.com

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

CHECKLISTE BEI DATENPANNEN

	Maßnahmen
	Es hat eine Datenpanne stattgefunden.
	Es sind Risiken für die Betroffenen zu erwarten (z. B. wenn Bankdaten offen gelegt wurden). Wenn ja, dann weiter mit folgenden Fragen ...
	Der Datenschutzbeauftragte oder -verantwortliche ist hinzuzuziehen.
	Es erfolgt eine Dokumentation des Vorfalls, einschließlich aller damit in Zusammenhang stehender Fakten, deren Auswirkungen und die ergriffenen Maßnahmen.
	Der Verantwortliche meldet den Vorfall innerhalb von 72 Stunden an die Behörde.
	Diese Meldung enthält folgende Informationen, die ggf. nachgereicht werden können: ✓ eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorie der Daten und der ungefähren Zahl der betroffenen Datensätze, ✓ den Namen und die Kontaktanschrift des Datenschutzbeauftragten, ✓ eine Beschreibung der wahrscheinlichen Folgen, ✓ eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Datenschutzverstoßes und ggf. Maßnahmen zur Milderung der möglichen Auswirkungen.
	Es muss eine Benachrichtigung der Betroffenen erfolgen, wenn die Datenpanne ein voraussichtlich hohes Risiko für die betroffene Person hat.
	Führen Sie eine Schwachstellenanalyse durch, um künftige Vorfälle zu vermeiden.

9 / DER DATENSCHUTZBEAUFTRAGTE IM UNTERNEHMEN

Compliance spielt besonders im Datenschutz eine wichtige Rolle, denn Online-Händler 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.

Das dürfte auf kleine und mittelständige Online-Händler nicht zutreffen, da sie kaum systematisch oder in größerem Umfang Kundendaten überwachen – zumindest nicht in der Hauptaufgabe. Aber Vorsicht: Ergänzend zur DSGVO muss ein Datenschutzbeauftragter nach deutschem Recht benannt werden, soweit sich **mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen**. Nur kleine Online-Händler sind damit auch weiterhin befreit.

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.

Auch wenn es für ihr Unternehmen (noch) keine Pflicht gibt, gelten alle anderen Vorschriften der DSGVO und sonstiger Datenschutzbestimmungen für Unternehmen. Unternehmer sollten daher jemanden festlegen, der die Verantwortung für die Einhaltung der Datenschutzbestimmungen übernimmt, und beurteilen, wo diese Rolle innerhalb der Struktur ihres Unternehmens angesiedelt ist.

10 / STRENGE AUFSICHT UND EFFEKTIVE RECHTSDURCHSETZUNG

Auch wenn Datenschutzverstöße in aller Munde sind. Beim Lesen der Pressemeldungen bekommt der Internetuser 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 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. Von besonderer Bedeutung für Online-Händler mit internationaler Ausrichtung dürfte das sogenannte „One-Stop-Shop Prinzip“ sein. Dies besagt, dass Bürger ihre Beschwerden immer an die Datenschutzbehörde ihres Mitgliedstaates richten müssen, ganz gleich, wo der Verstoß passiert ist. Gleiches gilt für Unternehmen: Auch diese müssen nur noch mit der für sie zuständigen Datenschutzbehörde zusammenarbeiten, also mit der des Mitgliedstaates, in dem sich ihr Hauptsitz befindet.

11 / 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 sog. „Verarbeitungsverzeichnis“ zu führen, welche die Datenverarbeitungsprozesse im Unternehmen katalogisiert.

Pflicht zur Erstellung eines Verarbeistungsverzeichnisses

Die Pflicht zur Führung eines Verarbeitungsverzeichnisses gilt nach der DSGVO nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Doch für jede Ausnahme gibt es natürlich eine Rückausnahme: Es gibt sehr wohl wieder eine Pflicht zur Führung eines Verarbeitungsverzeichnisses, wenn die Datenverarbeitung ein Risiko birgt, nicht nur „gelegentlich“ stattfindet und besondere Datenkategorien betroffen sind (z. B. bei Online-Apotheken, die Gesundheitsdaten verarbeiten). Obwohl es bisher keine nähere Definition von „gelegentlich“ gibt und kleinere und mittelständige Unternehmen vor einem erhöhten bürokratischen Aufwand geschützt werden sollen, kann die Pflicht auf Händler zutreffen. Schon die Hinterlegung von Kundeninformationen in der shopeigenen Datenbank erfolgt regelmäßig automatisch und nicht nur gelegentlich. Außerdem werten viele Shops systematisch das Verhalten ihrer Webseitenbesucher aus.

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:

- ✓ den Namen und die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten,
- ✓ die Zwecke der Datenverarbeitung,
- ✓ die 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 in Deutschland 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

Mit dem Fortschreiten der Technologisierung oder beim Wachstum des Unternehmens kommt es von Zeit zu Zeit zur Notwendigkeit, neue Datenverarbeitungsprozesse in das Unternehmen einzuführen. Hier wird einigen schon der Begriff der sog. Vorabkontrolle geläufig sein.

Nach der DSGVO muss der Verantwortliche künftig nur dann vorab seine Verarbeitungsprozesse behördlich überprüfen lassen, wenn die sog. 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 (sog. Folgenabschätzung). Dies ist insbesondere bei neuen Technologien der Fall, bei der Umfang und der Eingriff in die Persönlichkeitsrechte noch nicht feststeht. Die DSGVO nennt bestimmte Fallgruppen, bei denen eine Folgenabschätzung stets durchzuführen ist. Dazu zählen

- ✓ das Profiling,
- ✓ die Verarbeitung besonders sensibler Daten (z. B. Gesundheitsdaten)
- ✓ der Einsatz neuer Technologien
- ✓ die umfangreiche öffentliche Videoüberwachung.

BEISPIEL EINES VERARBEITUNGSVERZEICHNISSES

BEZEICHNUNG DER DATEN-VERABREITUNG	VERANTWORTLICHE(R)	VERANTWORTLICHER FACHBEREICH	BETROFFENE	KATEGORIEN VON DATEN
Kundenbetreuung	Muster-Online-Handels GmbH, vertreten durch den Geschäftsführer Max Mustermann	Kundenmanagement, Abteilungsleiter M. Muster	Bestandskunden, registrierte Webseiten-nutzer mit Kundenkonto	Name, Rechnungsad-resse, Lieferadresse, ausgelöste Bestellungen samt Zahlungsweise, Daten zur Sendungsver-folung, Schriftwechsel und Support-Anfragen, Abrechnungsdaten
Buchhaltung				
Vertrieb				

RECHTSGRUNDLAGE	EMPFÄNGER DER DATEN (INTERN/ EXTERN)	ÜBERMITTLUNG AN DRITTSTAATEN	MEDIUM DER DATENVERARBEITUNG	LÖSCHFRIST
Vertragsanbahnung bzw. Vertragsdurchführung	Kundenmanagement, Buchhaltung, ggf. Auskunftei XY zwecks Bonitätsprüfung	nein	Datenbankensoftware XY	nach Ablauf von handels-, steuerrechtlichen Aufbewahrungspflichten; bei Löschungsaufforderung durch Kunden; ansonsten ein Jahr nach Ablauf der Verjährungsfrist

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 „Verarbeitung“) personenbezogener Daten durch externe Dienstleister für den Auftraggeber (z. B. den Online-Händler).

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 dem Zweck der Datenverarbeitung geeignete Maßnahmen umzusetzen hat, um die Sicherheit der Daten zu gewährleisten (z. B. Verschlüsselung, Passwörter).

DATENSPARSAMKEIT

bedeutet, dass die Datenverarbeitung auf das notwendige Maß beschränkt sein muss, beispielsweise bei einer Bestellung im Online-Shop nur die Anschrift angefragt werden darf und nicht das Geschlecht.

DATENÜBERTRAGBARKEIT/ DATENPORTABILITÄT

ist der Anspruch einer Person, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Der Nutzer hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“.

DATENVERARBEITUNG

ist jeder Vorgang 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 Bereitstellung • den Abgleich oder die Verknüpfung • die Einschränkung • das Löschen oder die Vernichtung.

DRITTSTAATEN

sind Länder, die weder der Europäischen Union angehören noch zu den Staaten des Europäischen Wirtschaftsraumes zählen.

EINWILLIGUNG DER BETROFFENEN PERSON

ist jede unmissverständlich abgegebene Erklärung oder eindeutige Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist.

FOLGENABSCHÄTZUNG

ist die Abschätzung der Folgen für den Schutz personenbezogener Daten und muss durchgeführt werden, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten birgt.

KOHÄRENZVERFAHREN

ist die Befugnis des Europäischen Datenschutzausschusses, im Falle von Unstimmigkeiten zwischen den Aufsichtsbehörden verbindliche Beschlüsse zu treffen, um die ordnungsgemäße und einheitliche Anwendung der DSGVO sicherzustellen.

MARKTORTPRINZIP

besagt, dass ausländische Unternehmen nur dann Zugang zum europäischen Markt erhalten, wenn sie sich an die hier geltenden Regelungen halten.

ONE-STOP-SHOP

besagt, dass sich Unternehmen, die Niederlassungen in mehrere EU-Staaten haben und dort Daten verarbeiten, bei grenzüberschreitender Datenverarbeitung nur an die Aufsichtsbehörde an ihrem Hauptsitz wenden können.

PERSONENBEZOGENE DATEN

sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt mittels Zuordnung zu einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

PRIVACY BY DEFAULT

(Dt.: Datenschutz durch Voreinstellung) bedeutet, dass Produkte standardmäßig datenschutzfreundlich eingestellt sind (z. B. datenschutzfreundliche Voreinstellung eines Internet-Browsers).

PRIVACY BY DESIGN

(Dt.: Datenschutz durch technische Konstruktion) bedeutet, dass Unternehmen schon bei der Entwicklung und Konzeption ihrer (internen) Prozesse und Produkte (z. B. einer Software) dem Datenschutz und der DSGVO Rechnung tragen müssen.

PROFILING

ist jede automatisierte Verarbeitung personenbezogener Daten, um bestimmte personenbezogene Aspekte zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser Person zu analysieren oder vorherzusagen.

PSEUDONYMISIERUNG

ist die Verwendung von personenbezogenen Daten in einer Weise, in der diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

SENSIBLE DATEN

sind personenbezogenen Daten, aus denen die rassische und ethische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung.

VERANTWORTLICHER

ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Verarbeitung von personenbezogenen Daten entscheidet und für die Einhaltung der DSGVO sorgen muss.

VERARBEITUNGSVERZEICHNIS

katalogisiert die Datenverarbeitungsprozesse eines Unternehmens. Die Pflicht zur Führung eines Verarbeitungsverzeichnisses gilt nach der DSGVO nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Es gibt sehr wohl wieder eine Pflicht zur Führung eines Verarbeitungsverzeichnisses, wenn die Datenverarbeitung ein Risiko birgt, besondere Datenkategorien betroffen sind (z. B. bei Online-Apotheken die Gesundheitsdaten) und nicht nur „gelegentlich“ stattfindet.

VORABKONTROLLE

ist die Prüfung von Datenverarbeitungsvorgängen vor Beginn einer Datenverarbeitung.

ZWECKBINDUNG

heißt, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden dürfen, beispielsweise die E-Mail-Adresse nur für die Bestellbestätigung, nicht jedoch für Werbung verwendet werden darf.

IMPRESSUM

HERAUSGEBER

Händlerbund e. V.
Torgauer Straße 233
04347 Leipzig

VERLAG

Händlerbund Management AG
Torgauer Straße 233
04347 Leipzig
info@onlinehaendler-magazin.de

LAYOUT/SATZ

Franziska Vogel

REDAKTION

Ariane Nölte (Chefredakteurin);
Yvonne Bachmann (Rechtsanwältin);
Händlerbund Management AG
Torgauer Straße 233
04347 Leipzig
redaktion@onlinehaendler-magazin.de
yvonne.bachmann@haendlerbund.de

FAHRPLAN ZUR VORBEREITUNG AUF DIE DSGVO

1. Sensibilisierung und interne Datenschutzorganisation
2. Einen Datenschutzbeauftragten bzw. einen -verantwortlichen bestimmen
3. Eine Dateninventur durchführen, sog. Verarbeitungsverzeichnis
4. Mit neuen Auskunfts- und Betroffenenrechten vertraut machen
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

WEITERFÜHRENDE LINKS

Bayerisches Landesamt für Datenschutzaufsicht
Kurzpapiere der Datenschutzkonferenz (DSK), eigene Papiere und Anleitungen
https://www.lda.bayern.de/de/datenschutz_eu.html

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)
Studien, Stellungnahmen und Leitfäden
https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/index.jsp

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
diverse Praxishilfen
https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Informationen, Orientierungshilfen, Kontaktadressen der Landesdatenschutzbehörden
www.bfdi.bund.de

Händlerbund
Umfassende Infos und Hilfestellungen auf einen Blick
https://www.haendlerbund.de/de/leistungen/rechtssicherheit/agb-service/datenschutzgrundverordnung

KONTAKT

Händlerbund Management AG
Torgauer Straße 233
04347 Leipzig
Tel.: 0049 341 - 92 65 90
Fax: 0049 341 - 92 65 9100
Web: www.haendlerbund.de
Mail: info@haendlerbund.de

HÄNDLERBUND