www.buhl.de

DATENSCHUTZ KOMPAKT

Übersicht der wichtigsten Anforderungen aus EU-Datenschutzgrund-verordnung (EUDSGVO) und dem Bundesdatenschutzgesetz (BDSGneu)

BUHL

Hinweis: Diese Broschüre dient nur als eine grobe Übersicht und erhebt keinen Anspruch auf Vollständigkeit oder Richtigkeit.

INHALT

1 Einleitung 5

2 Die Grundsätze im Datenschutz 6

3 Ist Datenspeicherung überhaupt Zulässig? 7
3.1 Wie ist das mit besonderen „sensiblen" Daten? 8
3.2 Wie erfolgt eine „Einwilligung"? 9
3.3 Was ist beim Newsletter-Versand zu beachten? 10
3.4 Wie können wir die Einhaltung der Grundsätze nachweisen? 12

4 Pflichten gegenüber Kunden? 13
4.1 Informationspflichten 13
4.2 Auskunftpflichten 14

5 Wann dürfen Daten weitergegeben werden? 15
5.1 Datenweitergabe zur Vertragserfüllung 15
5.2 Datenweitergabe zur Erfüllung rechtlicher Verpflichtungen 15
5.3 Datenweitergabe bei „überwiegenden berechtigten Interessen" 16
5.4 Weitergabe von Kundendaten mittels Auftragsverarbeitung innerhalb der EU 16
5.5 Weitergabe von Kundendaten außerhalb der EU 16
5.6 Sonderfall USA 17

6 Wie dürfen Daten zu Werbezwecken genutzt werden? 18

7 Welche technischen Anforderungen sind zu beachten? 19
7.1 Privacy by Design (Datenschutz durch Technik) 19
7.2 Privacy by Default (Datenschutz durch Voreinstellungen) 19

8 Welche Rechte sind also zu beachten 20

9 Datenschutzverstöße 21

10 Beispiele: Was ist zulässig und was nicht 22

DSGVO

1 EINLEITUNG

Ab dem 25.5.2018 bricht in der EU ein neues Datenschutzzeitalter an. Ab diesem Tag gilt die neue Datenschutz-Grundverordnung (DSGVO). Gleichzeitig tritt ein neues Bundesdatenschutzgesetz in Kraft, welches ergänzende Regelungen für Deutschland enthält.

Das geltende Europäische Datenschutzrecht stammt aus dem Jahre 1995, mithin aus einer Zeit, als das Internet noch in den Kinderschuhen steckte und die automatisierte Datenverarbeitung kaum in vernetzten Systemen stattfand. Angesichts der Digitalisierung sämtlicher Lebensbereiche, der globalen Datenverarbeitung und der damit verbundenen allgegenwärtigen Erfassung, Speicherung, Auswertung und Profilbildung unseres Handelns und Denkens bedarf das in die Jahre gekommene Recht einer Modernisierung. Zudem bedarf das Europäische Datenschutzrecht einer stärkeren Harmonisierung. Die zurzeit bestehende Landschaft aus 28 verschiedenen Datenschutzgesetzen ist angesichts grenzüberschreitender Datenverarbeitung sowohl für die Bürgerinnen und Bürger, als auch für die Anwender hinderlich. Die Verarbeitung personenbezogener Daten macht weder vor nationalen noch vor kontinentalen Grenzen halt. Unternehmen aus der ganzen Welt sind auf dem Europäischen Markt tätig und verarbeiten unsere Daten, ohne dass sie sich durchgängig an das Europäische Datenschutzrecht halten müssen.

Der Datenschutz kann den Einzelnen nicht vor jeglicher Form von Verarbeitung seiner Daten bewahren, aber er soll es ihm ermöglichen, grundsätzlich selbst darüber zu bestimmen, „wer was über ihn weiß".

„Zweck dieser Gesetze ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."

Diese Informationsbroschüre will dazu beitragen, das Datenschutzrecht verständlich darzustellen.

2 DIE GRUNDSÄTZE IM DATENSCHUTZ

Die DSGVO sieht eine Vielzahl von allgemeinen Grundsätzen vor, die in diesem Artikel näher beschrieben werden.
Die allgemeinen Grundsätze stellen dabei so etwas wie die „Grundregeln" für die Verarbeitung von personenbezogenen Daten dar.

Rechtmäßigkeit der Verarbeitung

Die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn eine Einwilligung vorliegt oder eine sonstige Rechtsgrundlage dies zulässt.

Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen sein, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.

Zweckbindung

Personen müssen über den Zweck der Verabeitung der Daten informiert werden. Die erhobenen Daten dürfen auch nur zu diesem Zweck genutzt werden.

Integrität und Vertraulichkeit

Zur Sicherung der Daten sind technische und organisatorische Maßnahmen zu treffen, die den Schutz gewährleisten.

Transparenz

Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.

Richtigkeit der Daten

Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sollen unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck nicht mehr erforderlich ist, so müssen die personenbezogenen Daten gelöscht werden.

3 IST DATENSPEICHERUNG ÜBERHAUPT ZULÄSSIG?

Grundsätzlich erstmal NEIN!

Grundsätzlich ergibt sich aus dem Grundrecht auf informationelle Selbstbestimmung zunächst ein Verbot, wonach jedwedes Erheben, Verarbeiten und/oder Nutzen von personenbezogenen Daten verboten ist (Regel), es sei denn ein Gesetz oder die Einwilligung des Betroffenen rechtfertigen (Ausnahme) dies.

Allgemein spricht man auch vom Verbotsprinzip mit Erlaubnisvorbehalt.
Wann darf ich also Kundendaten verarbeiten?

Die Verarbeitung von Kundendaten ist nur erlaubt bei:

- Einwilligung
- Erforderlichkeit zur Durchführung eines Vertrags
- Erforderlichkeit zur Durchführung vorvertraglicher Maßnahmen (z.B. Download einer Trial-Version, Angebot)
- Anderen Rechtspflichten oder nach einer Interessenabwägung

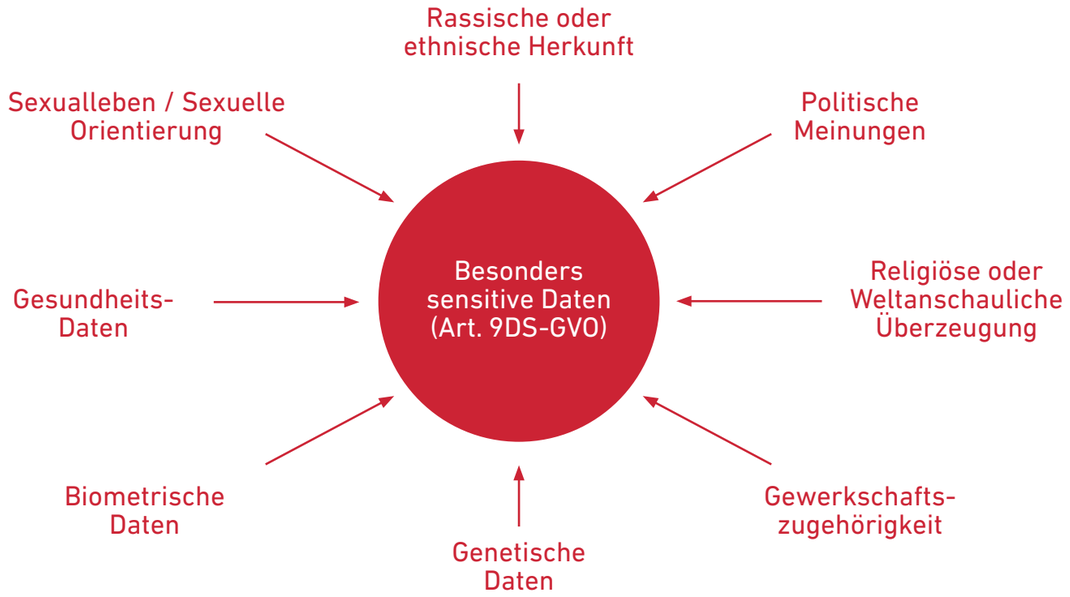
Wenn ein Kunde also einen Vertrag abschließt, z.B. durch Kauf eines Produkts, darf man seine dazu notwendigen Daten auch speichern. Für alle anderen Daten benötigt man üblicherweise seine Einwilligung, d.h., er muss diese Daten freiwillig geben.

Unter personenbezogenen Daten (pbD) versteht man alle Informationen, mit der sich eine Person bestimmen lässt.
Das sind beispielsweise: Name, Alter, Familienstand, Geburtsdatum, An-schrift, Telefonnummer, E-Mail-Adresse, Konto-, Kreditkartennummer, Kraftfahrzeugnummer, Kfz-Kennzeichen, Personalausweisenummer, Sozialausweisnummer, aber auch die IP-Adresse!

3.1 WIE IST DAS MIT BESONDEREN „SENSIBLEN“ DATEN?

Die Verarbeitung solcher sensiblen Daten ist grundsätzlich verboten, da sie sich durch eine große Sensibilität kennzeichnen. Hier muss sich die Einwilligung ausdrücklich auf diese Daten beziehen, weshalb darauf zu achten ist, dass eine Einwilligung vor der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten vorliegt.

Ein besonderer Schutz gilt für diese Daten:



3.1 WIE ERFOLGT EINE „EINWILLIGUNG“?

Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bedarf grundsätzlich einer Einwilligung, wenn keine besondere gesetzliche Ausnahme (z.B. ein Vertrag) vorliegt. Danach gilt:

- ✔ Eine Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, d. h. sie muss freiwillig erfolgen.
- ✔ Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.
- ✔ Die Einwilligung bedarf grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.
- ✔ Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Einwilligungen erfolgen zunehmend in elektronischer Form.
Dies ist möglich, wenn sicherstellt wird, dass .

- ✔ der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- ✔ die Einwilligung protokolliert wird,
- ✔ der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- ✔ der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann (und hierauf hingewiesen wird).

Eine personenbezogene Speicherung darf zudem nur für festgelegte Zwecke erfolgen.

3.3 WAS IST BEIM NEWSLETTER-VERSAND ZU BEACHTEN?

1. Man benötigt eine Einwilligung (außer bei Direktwerbung)
2. Die Einwilligung muss über ein Double-Opt-IN eingeholt werden
3. Die Einwilligung muss protokolliert werden, da eine Nachweispflichtig besteht.
4. Man darf nur die Daten erheben, die für den Erhalt eines Newsletters notwendig sind (Datenminimierung)
5. Die Einwilligungserklärung sollte enthalten (Transparenz):
   - Art der beabsichtigten Werbung (Brief, E-Mail/SMS, Telefon, Fax)
   - Produkte oder Dienstleistungen, für die geworben werden soll
   - Häufigkeit des Versands (z.B. „in der Regel monatlich“)
   - das werbende Unternehmen
6. Es muss ein Hinweis auf eine Widerrufsmöglichkeit gegeben werden, auch in jedem Newsletter
7. Die Bestätigungs-E-Mail muss stets absolut werbefrei sein
8. Aus Kopf- und Betreffzeile muss sich der Absender und kommerzielle Charakter ergeben
9. In der Bestätigungs-E-Mail muss die komplette Einwilligung enthalten sein.
10. Für die Pflichtinformationen ist ein Link zur Datenschutzerklärung notwendig.

BEISPIEL:

☐ Ja, ich möchte von xy-GmbH in der Regel einmal im Monat kostenfrei Newsletter und Informationen über Leistungen, Updates und Service-Packs per E-Mail erhalten.

***E-Mail:**

Für eine persönliche Anrede füllen Sie bitte auch folgende Felder aus:

Anrede:

Vorname:

Name:

Hinweis: Sie erhalten nach Ihrer Anmeldung eine E-Mail mit Bestätigungslink. Bitte bestätigen Sie diesen, damit Sie in unseren Verteiler aufgenommen werden.

Abmeldung/Widerruf

Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, indem Sie in Ihrem „Kundencenter“ unter www.xy.de den Newsletter abwählen. Wahlweise klicken Sie auf den Link zum Abbestellen am Ende eines jeden Newsletters. Hierfür entstehen Ihnen keine Kosten. Weitere Infos finden Sie hier in unserer Datenschutzerklärung.

3.4 WIE KANN DIE EINHALTUNG DER GRUNDSÄTZE NACHGEWIESEN WERDEN?

Hier werden von den Verantwortlichen (dies sind die Personen, die über eine Datenspeicherung entscheiden) 2 wichtige Nachweise verlangt:

1. Datenschutzfolgenabschätzung

Ein Verantwortlicher ist immer in der Pflicht, Risiken bei der Verarbeitung zu berücksichtigen und zu dokumentieren. Diese Pflicht besteht aber auch, wenn keine hohen Risiken vorliegen.

Die DSGVO verpflichtet aber die Verantwortlichen, eine sog. Datenschutz-Folgenabschätzung (DSFA) vorzunehmen, wenn ein „voraussichtlich hohes Risiko" mit der Verarbeitung von Daten verbunden ist.

Beispiele für ein „hohes Risiko" sind:

- ✔ Videoüberwachung
- ✔ Verarbeitung biometrischer Daten
- ✔ Verarbeitung von Gesundheitsdaten
- ✔ Umfangreiche Datenverarbeitungen

2. Verarbeitungsverzeichnis

Die DSGVO verlangt eine Beschreibung zu jedem Datenverarbeitungsverfahren, mit dem personenbezogene Daten gespeichert werden.

Da die Speicherung personenbezogener Daten grundsätzlich verboten ist, geht es bei dem Verzeichnis darum, den Erlaubnistatbestand schriftlich festzuhalten und wie die Daten geschützt werden.

Der Inhalt ist vorgegeben und muss insbesondere die technisch-organisatorischen Maßnahmen auflisten. Das Verzeichnis ist der Aufsichtsbehörde auf Verlangen vorzulegen, sonst kann ein Bußgeld bis 10 Mio. € verhängt werden.

4 PFLICHTEN GEGENÜBER KUNDEN

4.1 INFORMATIONSPFLICHTEN

Die Datenschutz-Grundverordnung (DSGVO) legt größten Wert auf die Transparenz im Zusammenhang mit der Verarbeitung personenbezogener Daten. So sollen zum Zeitpunkt der Erhebung verpflichtend eine Reihe an Angaben gemacht werden, welche die betroffenen Personen über die Datenverarbeitung und deren Zwecke in Kenntnis setzen.
Die DSGVO verlangt dabei mindestens die folgenden (sage und schreibe) 12 Aussagen:

- ✔ Name und Kontaktdaten des Datenverarbeiters
- ✔ Kontaktdaten des Datenschutzbeauftragten des Datenverarbeiters
- ✔ Zweck(e) der Verarbeitung
- ✔ Die „berechtigten Interessen" im Sinne der DSGVO, sofern sich hierauf seitens des Datenverarbeiters berufen wird
- ✔ Die Empfänger der erhobenen Daten (z.B. Auftragsverarbeiter der erhebenden Stelle)
- ✔ Die Absicht, die Daten in einen Staat außerhalb der EU zu übermitteln, sofern diese besteht
- ✔ Die Dauer der Speicherung, im Umkehrschluss auch den regelmäßigen Löschzeitpunkt
- ✔ Eine Belehrung der betroffenen Person über ihre Rechte (Auskunft, Löschung etc.)
- ✔ Die Widerruflichkeit einer Einwilligung, sofern die Verarbeitung auf einer solchen basiert
- ✔ Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ✔ Ggf. bestehende gesetzliche Vorschriften zur Bereitstellung der erhobenen Daten
- ✔ Ggf. Informationen zum Bestehen einer „automatisierten Einzelentscheidung" im Kontext der jew. Verarbeitung

Im Regelfall erfolgt diese Informationen durch eine Datenschutzerklärung.
Daher muss diese immer (mit 1-Klick) erreichbar sein.

4.2 AUSKUNFTSPFLICHTEN

Das Auskunftsrecht ist aus datenschutzrechtlicher Sicht keine Neuigkeit. Werden personenbezogene Daten verarbeitet, hat der Betroffene grundsätzlich ein Recht auf Auskunft über diese Daten. Zusätzlich hat der Verantwortliche auch die folgenden Informationen bereitzustellen:

- ✔ Verarbeitungszwecke
- ✔ Kategorien personenbezogener Daten, die verarbeitet werden
- ✔ Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig erhalten werden
- ✔ geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer
- ✔ Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung
- ✔ Widerspruchsrecht gegen diese Verarbeitung
- ✔ Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde
- ✔ Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden
- ✔ das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren
- ✔ Werden personenbezogene Daten in Drittländer übermittelt, haben betroffene Personen darüber hinaus das Recht, über die in Zusammenhang mit der Datenübermittlung getroffenen geeigneten Garantien (z.B. vereinbarte Standard-Datenschutzklauseln oder verbindliche interne Datenschutzvorschriften) informiert zu werden.

Auf Anfrage müssen Kunden diese Informationen innerhalb eines Monats zur Verfügung gestellen werden!

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

5 WANN DÜRFEN DATEN WEITERGEGEBEN WERDEN?

Im Unternehmensalltag ist es kaum vorstellbar, keine Daten mit anderen auszutauschen. Daten werden an Lieferanten weitergegeben, von Adresshändlern für Marketingzwecke eingekauft, zentrale Stellen innerhalb einer Konzerngruppe erbringen Personaldienstleistungen für alle Konzernunternehmen, die IT-Hotline ist u. a. in Indien angesiedelt oder Daten werden kostengünstig in den USA gespeichert — um nur einige Beispiele zu nennen.

Eine Weitergabe von Kundendaten an Dritte darf nur mit Einwilligung des Betroffenen oder auf Grundlage einer gesetzlichen Erlaubnis erfolgen.

5.1 DATENWEITERGABE ZUR VERTRAGSERFÜLLUNG

Ist die Weitergabe für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich, so ist dies ohne eine Einwilligung des Kunden zulässig. Dies kann etwa die Weitergabe der Kundendaten an ein Versandunternehmen oder das Zahlungsinstitut beinhalten. Jedoch gilt auch hier das Prinzip der Datensparsamkeit, d.h. der Umfang der Daten muss sich auf das mögliche Minimum beschränken.

5.2 DATENWEITERGABE ZUR ERFÜLLUNG RECHTLICHER VERPFLICHTUNGEN

Wenn spezielle Gesetze dies vorschreiben, dürfen z.B. Daten an die Finanzbehörden übermittelt werden, sofern dies aus steuerrechtlichen Gründen erforderlich ist.

5.3 DATENWEITERGABE BEI „ÜBERWIEGENDEN BERECHTIGTEN INTERESSEN“

Danach dürfen Daten immer dann, wenn berechtigte Interessen des Unternehmens vorliegen, die gegenüber den schutzwürdigen Interessen des Betroffenen überwiegen, weitergegeben werden. Dies kann z.B. den Austausch von Daten innerhalb einer Unternehmensgruppe rechtfertigen (Lohnabrechnung für Tochterunternehmen).

5.4 WEITERGABE VON KUNDENDATEN MITTELS AUFTRAGSVERARBEITUNG INNERHALB DER EU

Von Auftragsdatenverarbeitung ist die Rede, wenn Unternehmer die Verarbeitung personenbezogene Daten aus ihrem Unternehmen an Externe weitergeben. Dies ist z.B. bei der Zusammenarbeit mit Inkasso-, Versand- oder Logistik-Dienstleistern der Fall. Hierbei wird der Auftragnehmer nicht als Dritter, sondern als “verlängerter Arm” des Auftraggebers gewertet, sodass keine gesonderte Einwilligung in die Weitergabe notwendig ist.

Ein solcher Vertrag kann ausschließlich schriftlich geschlossen werden und muss diverse Voraussetzungen erfüllen, weshalb eine Rechtsberatung und ein Datenschutzbeauftrager hinzugezogen werden sollten.

5.5 WEITERGABE VON KUNDENDATEN AUSSERHALB DER EU

Eine Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR kann rechtmäßig nur dann erfolgen, wenn im Drittland ein angemessenes Datenschutzniveau gewährleistet ist. Hierzu gibt es eine Liste mit Ländern, bei denen die EU-Kommission dies bestätigt hat. Dazu gehören z.B. Kanada, Neuseeland, Schweiz, aber nicht USA. Eine Datenübermittlung in solche Länder ist also möglich, sofern der Kunde hierüber informiert wird und ihm eine Widerspruchsmöglichkeit gegeben wird, ggf. ist auch eine Vereinbarung zur Auftragsverarbeitung erforderlich.

5.6 SONDERFALL USA

Die USA sind kein Staat mit angemessenem Datenschutzniveau. Vor eine Datenübermittlung in die USA müssen daher geeignete Garantien geschaffen werden, die den Mangel an Datenschutz ausgleichen. Dies können sein:

- ✔ EU-Standarddatenschutzklauseln. Diese sind von der EU-Kommission herausgegeben und das US-Unternehmen muss diese rechtlich bindend unterschreiben.
- ✔ Ein eigener Vertrag, der jedoch von der Aufsichtsbehörde genehmigt werden muss
- ✔ Genehmigte Verhaltensregeln, z.B. der EU-US Datenschutzschild (Privacy Shield). Das Privacy Shield ist eine „Angemessenheitsentscheidung“ der EU-Kommission. Eine Datenübermittlung an Unternehmen, die sich an den Privacy Shield gebunden haben, ist also möglich, sofern der Kunde hierüber informiert wird und ihm eine Widerspruchsmöglichkeit gegeben wird.

In jedem Fall müssen diese Garantien vor Einsatz einer Datenübertragung in die USA geschaffen werden.

6 DÜRFEN DATEN ZU WERBE-ZWECKEN GENUTZT WERDEN?

Die bisherigen detaillierten Regelungen zur erlaubten Werbung entfallen mit der DSGVO, so auch das „Listenprivileg". Im Prinzip ändert sich mit der DSGVO zumindest hinsichtlich der Verwendung von Datenmaterial für Werbezwecke nicht viel. Die Regeln des UWG bleiben maßgebend für Werbung. Paragraph 7 UWG regelt, was als unzumutbare Belästigung eingestuft wird und damit unrechtmäßig ist. Postalische Werbung stellt kein Problem dar, solange der Betroffene eine Möglichkeit zur Abmeldung hat. Werbung per Fax oder E-Mail ist gleichermaßen untersagt, wenn keine explizite Einwilligung oder kein Kundenverhältnis vorliegt. Bei Telefonwerbung wird nach Firmen und Privatpersonen unterschieden. Für Privatpersonen gelten genauso strikte Regelungen wie für Fax und E-Mail, und bei Firmen genügt eine „mutmaßliche Einwilligung".

Künftig müssen Verarbeitungen personenbezogener Daten zu Zwecken der Werbung daher entweder auf einer Einwilligung basieren oder auf dem recht unspezifisch formulierten Artikel 6 Abs. 1 lit. f DS-GVO. Nach dieser Regelung ist zwischen den berechtigten Interessen des Verantwortlichen und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person abzuwägen.
Wann liegt aber eine Wahrung der berechtigten Interessen vor? Hier spielen die sogenannten Erwägungsgründe (ErwGr.) eine Rolle. Mit diesem Instrument schaltet der europäische Gesetzgeber in Richtlinien und Verordnungen Auslegungshilfen vor. In Erwägungsgrund 47 wird ausgeführt:

„Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Dieser „kann-Satz" wird künftig die eigentliche datenschutzrechtliche Grundlage für die Werbung sein.

Zu beachten ist, dass die von Werbung betroffenen Personen ein jederzeitiges und umfassendes Widerspruchsrecht haben, auf das sie ausdrücklich hinzuweisen sind. Danach können Betroffene die Verwendung ihrer Daten für Werbezwecke jederzeit stoppen lassen.

7 WELCHE TECHNISCHEN ANFORDERUNGEN SIND ZU BEACHTEN?

Schon bei der Konzeption von IT- und Datenverarbeitungssystemen sind 2 Hauptziele des Datenschutzes zu gewährleisten:

7.1 PRIVACY BY DESIGN (DATENSCHUTZ DURCH TECHNIK)

Hard- und Software sollen bereits datenschutzfreundlich entwickelt und nicht erst nachträglich „aufgerüstet" werden. Hinter „Privacy by Design" steckt der Gedanke, dass sich Verstöße gegen das Datenschutzrecht eher vermeiden lassen, wenn datenschutzrechtliche Anforderungen schon im Entwicklungsprozess berücksichtigt werden. Privacy by Design bedeutet auch, dass die Regelungen des Datenschutzes bereits bei der Produktentwicklung berücksichtigt werden und durch geeignete technische und organisatorische Maßnahmen, wie z.B. Pseudonymisierung und Verschlüsselung, die im Datenschutzrecht geltenden Grundsätze der Datenvermeidung und Datensparsamkeit eingehalten werden müssen.

7.2 PRIVACY BY DEFAULT (DATENSCHUTZ DURCH VOREINSTELLUNGEN)

Hard- und Software soll datenschutzfreundliche Grundeinstellungen haben. Nutzer sollen dann in einem zweiten Schritt entscheiden können, ob und wie ihre Daten genutzt werden dürfen.

8 WELCHE RECHTE SIND ALSO ZU BEACHTEN

Betroffenenrechte beschreiben das Recht der von der Datenverarbeitung betroffenen Personen. Ihnen stehen im Vorfeld, während und nach der Datenverarbeitung zahlreiche Rechte zu Verfügung.

- ✔ Das vielleicht wichtigste Betroffenenrecht im Rahmen der DSGVO stellt das Informationsrecht des Betroffenen dar.
- ✔ Dem Informationsrecht korrespondiert ein Auskunftsrecht des Betroffenen. Dieser kann in angemessenen Abständen Auskunft über die Datenverarbeitung, v.a über den Zweck, darüber welche Daten verarbeitet werden und über den Empfänger verlangen.
- ✔ Resultiert eine Datenverarbeitung in unrichtigen personenbezogen Daten des Betroffenen, so hat dieser ein Recht auf unverzügliche Berichtigung
- ✔ „Das Recht auf Vergessenwerden". Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen. Allerdings gibt es dazu ein paar Ausnahmen, z.B. wenn eine gesetzliche Aufbewahrungsfrist besteht.
- ✔ Das Recht auf Datenübertragbarkeit ist ein gänzlich neues, erst durch die DSGVO geschaffenes Recht. Es beinhaltet für den Betroffenen die Möglichkeit gespeicherte Daten (v.a. bei sozialen Medien) automatisch auf einen anderen Anbieter übertragen zu lassen.
- ✔ Das Recht auf Einschränkung der Verarbeitung. Der Betroffene hat unter bestimmten Bedingungen ein Recht auf Einschränkung der Verarbeitung, d.h. auf ein „Stopp!" der Verarbeitung.
- ✔ Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
- ✔ Jeder hat das Recht auf Beschwerde bei einer Aufsichtsbehörde
- ✔ Vervollständigt wird das Kapitel der Betroffenenrechte in der DSGVO schließlich durch das Widerspruchsrecht.

9 DATENSCHUTZVERSTÖSSE

Wird bei der Datenverwendung der Schutz personenbezogener Daten verletzt, muß das der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden gemeldet werden. Bei Verdacht sollten Sie sich daher umgehend an Ihre Rechtsberatung und/oder Ihren Datenschutzbeauftragten wenden.

Bei schwerwiegenden Verstößen gegen das Datenschutzrecht können Geldbußen bis zu 20 Mio.Euro verhängt werden!

10 BEISPIELE: WAS IST ZULÄSSIG UND WAS NICHT?

Ein Kunde kauft eines Ihrer Produkte, und Sie speichern die Kundendaten. Zulässig, da die Datenverarbeitung auf Grund einer Vertragsbeziehung erfolgt

Sie wollen einen Kunden anrufen, um ihn auf ein neues Produkt aufmerksam zu machen. Unzulässig, Werbung per Telefon wird grundsätzlich als Belästigung gesehen, außer der Kunde hat vorher eine Einwilligung gegeben.

Ihre Personalabteilung übermittelt Lohn- und Einkommensdaten an das Sozialamt. Zulässig, da das Steuer- und Sozialversicherungsgesetz dies vorschreibt.

Ihr Unternehmen stellt ein Mitarbeiterfoto auf eine Internetseite. Nur zulässig, wenn der Mitarbeiter eingewilligt hat.

Sie schicken einem Kunden Werbung zu einem neuen Produkt. Der Kunde hat aber früher jeglicher Werbung widersprochen. Unzulässig, bei einem Werbewiderspruch dürfen Kundendaten für den Zweck „Werbung" nicht mehr genutzt werden.

Jemand hat Ihnen auf einer Messe seine Visitenkarte gegeben und Sie wollen ihn zu dem besprochenen Produkt anrufen. Zulässig im B2B, da Sie von einem mutmaßlichen Interesse ausgehen können.

Jemand hat Ihnen auf einer Messe seine Visitenkarte gegeben und Sie tragen ihn für Ihre Newsletter ein. Unzulässig, da die Visitenkarte keine Einwilligung in Werbung darstellt. Zulässig, wenn der Kunde auf der Rückseite notiert hat „Bitte senden Sie mir Newsletter zu Ihren Produkten".

Sie beauftragen ein externes Unternehmen mit der Erstellung und Etikettierung von Versandaufklebern zum Versenden von Produkten. Nur zulässig, wenn mit diesem Unternehmen vorher ein Vertrag abgeschlossen wurde, in dem das Unternehmen Datenschutz zusichert.

Für den Download eines Gratis-Whitepapers verlangen Sie die Bekanntgabe von deutlich mehr Daten, als nur eine E-Mail-Adresse zur Übermittlung eines Download-Links. Unzulässig, da der Kunde mit seinen Daten quasi „bezahlen" soll. Damit wäre dies eine erzwungene Einwilligung und somit unwirksam.

© Copyright 2018 Buhl Data Service GmbH

Alle Rechte vorbehalten. Nachdruck, auch auszugsweise, verboten. Kein Teil dieses Werkes darf ohne schriftliche Einwilligung der Buhl Data Service GmbH in irgendeiner Form (Fotokopie, Mikrofilm, Scan oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Änderungen, Irrtümer und Druckfehler vorbehalten.