

Rechtsberatung	Steuerberatung	Beratung für Unternehmen & Vereine
<ul style="list-style-type: none">· Zivilrecht· Arbeitsrecht· Medizinrecht· Ordnungswidrigkeiten/ Strafrecht· Öffentliches Recht	<ul style="list-style-type: none">· Steuerberatung· Steuergestaltung· Vertretung vor den Finanzgerichten	<ul style="list-style-type: none">· Beratung relevanter Rechtsgebiete· Beratung und Betreuung von Unternehmensgründungen, -führungen, -nachfolgen· Betriebswirtschaftliche Beratung

Tieckstraße 2 · 14469 Potsdam · Telefon: 0331.201 48 30 · Telefax: 0331.201 48 38
E-Mail: sekretariat@kraft-friederich.de · www.kraft-friederich.de

Datenschutz-Grundverordnung DSGVO 2018

Am 25. Mai 2018 tritt die neue Datenschutzgrundverordnung (DSGVO) der Europäischen Union oder auch die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ in Kraft. Doch was bedeutet das für mich als Unternehmer, für meine Firma, meinen Verein, meine Webseite? Was muss ich beachten und welche Pflichten gehen mit dieser Verordnung für mich einher?

Bisherige Rechtslage:

Bis zum Inkrafttreten der neuen DSGVO galt für die Mitgliedstaaten der Europäischen Union die EU-Richtlinie 95/46 EG aus dem Jahre 1995. In Zeiten von sozialen Netzwerken wie Facebook, Twitter & Co. und der Digitalisierung nahezu aller Lebensbereiche, wuchs das Bedürfnis nach einem einheitlichen europaweiten Datenschutz. Die Zeiten haben sich im Hinblick auf die Verarbeitung personenbezogener Daten erheblich verändert, so dass die Richtlinie aus dem Jahre 1995 nicht mehr der heutigen Zeit entsprach und nicht dem Erfordernis nach einem umfassenden Datenschutz gerecht wurde.

Neben der europaweit geltenden DSGVO gilt in Deutschland auch das Bundesdatenschutzgesetz (BDSG). Das BDSG überträgt EU-Datenschutzrecht in nationales Recht. Daneben verfügt auch jedes Bundesland über ein eigenes Datenschutzgesetz.

Welchen Zweck verfolgt die DSGVO?

Die Rechte natürlicher Personen, also der Verbraucher, im Umgang mit ihren sensiblen personenbezogenen Daten sollen gestärkt und der Schutz dieser Daten erweitert werden. Unternehmer, Betreiber von Internetseiten und alle sonstigen Datenverarbeiter sollen und müssen mehr Verantwortung im Umgang mit personenbezogenen Daten übernehmen. Zugleich sollen die Rechte des Betroffenen gestärkt werden und mehr Transparenz für diesen geschaffen werden. Jeder soll das Recht haben, Auskunft darüber zu erlangen, welche Daten, in welchem Umfang, zu welchem Zweck, von wem erhoben, gespeichert oder sonst verarbeitet wurden.

Die wichtigsten Regelungen der DSGVO:

Doch was bedeutet die neue DSGVO nun für mich? Was muss ich beachten? Welche Pflichten obliegen mir oder meinem Unternehmen? Welche Rechte hat mein Kunde bzw. Nutzer?

Im Folgenden sollen die wesentlichsten Rechte und Pflichten im Umgang mit personenbezogenen Daten nach der DSGVO erläutert werden:

1. Bin ich von der DSGVO betroffen?

Die DSGVO regelt ihren sachlichen und räumlichen Anwendungsbereich selbst in Art. 2 und 3 DSGVO. Hierbei ist ganz abstrakt geregelt, dass die DSGVO überall da ihre Anwendung findet, wo personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden oder auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der räumliche Geltungsbereich der Verordnung erstreckt sich auf das Gebiet der Europäischen Union und seiner Mitgliedstaaten.

Doch was heißt das nun im konkreten Fall für mich und mein Unternehmen/Verein etc.:

Betroffen sind Betreiber von Internetseiten, Vereine (Sportvereine etc.), Verbände, Unternehmen, die Kundendaten speichern und verwalten, Schulen, Onlineshop-Betreiber, Ärzte, Rechtsanwälte, Handwerksbetriebe, also jeder, der irgendwie personenbezogene Daten verarbeitet.

Die DSGVO gilt also für alle natürlichen Personen, öffentliche Institutionen und Privatunternehmen, die ihren Sitz in der EU haben und im Rahmen ihrer betrieblichen oder unternehmerischen Tätigkeit mit personenbezogenen Daten arbeiten.

2. Was sind denn eigentlich personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar meint, dass mittels Zuordnung zu einem Namen, einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem anderen besonderen Merkmalen eine Person identifiziert werden kann.

Dazu gehören also insbesondere: Name, Adresse, Geburtsdatum, Geschlecht, Staatsangehörigkeit, Herkunft, Alter, Kleidergröße, IP-Adressen, E-Mail-Adresse, Kontaktdaten, politische Meinung,

religiöse Überzeugungen etc.. Man könnte sagen, personenbezogene Daten sind all die Daten, die die Person als Individuum und als Menschen, als Persönlichkeit ausmachen.

3. Welche personenbezogenen Daten dürfen verarbeitet werden?

Bestimmte personenbezogene Daten sind besonders schutzwürdig und dürfen daher nur in bestimmten Ausnahmefällen verarbeitet werden.

Hierzu zählen personenbezogene Daten über:

- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten o. Daten zum Sexualleben o. der sexuellen Orientierung einer natürlichen Person.

Diese Daten dürfen **grundsätzlich nicht** verarbeitet werden.

Ausnahmsweise dürfen auch diese Daten verarbeitet werden wenn:

- der Betroffene für einen oder mehrere festgelegte Zwecke ausdrücklich in die Verarbeitung solcher Daten eingewilligt hat oder
- die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

4. Wann spricht man von Datenverarbeitung?

Verarbeitung meint das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

Datenverarbeitung ist also nach der DSGVO sehr weit gefasst und umfasst nahezu jede denkbare Verarbeitung mit personenbezogenen Daten von der Erhebung bis zur Löschung der Daten und darüber hinaus.

5. Welche Pflichten habe ich ab dem 25.05.2018?

5.1. Zweckgebundene Datenverarbeitung:

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Das heißt, Sie müssen nachweisen können, zu welchem Zweck Sie personenbezogene Daten verarbeiten.

Personenbezogene Daten dürfen nur in dem Maß verarbeitet werden, wie es für die Verfolgung des Zweckes notwendig ist. Bsp.: Das Speichern des Geburtsdatums ist erforderlich, wenn zur Verfolgung des Zweckes gewährleistet sein muss, dass der Kunde/ Nutzer volljährig ist.

Eine Identifizierung des Betroffenen darf nur solange möglich sein, wie es für die Verfolgung des Zweckes erforderlich ist. Das ist beispielsweise dann nicht mehr der Fall wenn ein Vereinsmitglied aus dem Verein austritt oder ein Nutzer seinen Account auf ihrer Webseite kündigt/ löscht o.ä..

5.2. Pflicht zur korrekten Erfassung, Berichtigung und Löschung von Daten:

Die personenbezogenen Daten müssen sachlich richtig erfasst sein. Sofern sie unrichtig sind, müssen sie berichtigt oder gelöscht werden (Anspruch des Betroffenen auf Richtigkeit). Teilt Ihnen der Betroffene also mit, dass bestimmte personenbezogene Daten über ihn unrichtig erfasst wurden oder nicht mehr zutreffen, sind Sie verpflichtet, diese zu berichtigen.

Unrichtige und unzutreffende Daten müssen gelöscht werden. Darüber hinaus hat der Betroffene das Recht, jederzeit die Löschung personenbezogener Daten zu verlangen („Recht auf Vergessenwerden“).

5.3. Pflicht zum Schutz der Daten und Meldepflicht:

Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen vor dem unberechtigten und unbefugten Zugriff und der Verarbeitung durch Dritte geschützt werden, sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Welche konkreten Maßnahmen zum Schutz der Daten erforderlich sind (wie bspw. Datenverschlüsselung), sollte durch entsprechendes Fachpersonal (Techniker, IT-Fachleute usw.) geklärt werden. Lassen Sie sich hierzu daher von entsprechenden Fachkräften beraten.

Im Falle einer Verletzung des Schutzes personenbezogener Daten sind Sie verpflichtet, den Betroffenen unverzüglich und möglichst binnen 72 Stunden, nachdem Ihnen die Verletzung bekannt wurde, zu melden. Das ist beispielsweise der Fall, wenn Sie Kenntnis darüber erlangen, dass ein Dritter unberechtigt Zugriff auf die personenbezogenen Daten erlangt hat.

5.4. Wann und unter welchen Umständen bin ich berechtigt Daten zu verarbeiten?

Die Datenverarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- a) Die betroffene Person hat ihre **Einwilligung** in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

So abstrakt regelt es Art. 6 der DSGVO. Das heißt, die Einwilligung des Betroffenen in die Datenverarbeitung muss zwar nicht in jedem Fall eingeholt werden, wenn eine der anderen Alternativen erfüllt ist. Dennoch ist es ratsam, sich vorsorglich die Einwilligung zur Datenverarbeitung von dem Betroffenen einzuholen. Hierdurch können Sie etwaigen Rechtsstreitigkeiten vorbeugen.

5.5. Pflicht zum Nachweis der Einwilligung und die Einwilligung Minderjähriger:

Sie müssen stets nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Es muss klar sein, für welchen konkreten Sachverhalt die Einwilligung erteilt wurde. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.

Das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung personenbezogener Daten beträgt 16 Jahre, d.h. der/ die Betroffene kann die Einwilligung in die Verarbeitung nur dann wirksam erteilen, wenn er /sie das 16. Lebensjahr vollendet hat. Hat das Kind noch nicht das 16. Lebensjahr vollendet, so ist die Einwilligung oder Zustimmung des gesetzlichen Vertreters erforderlich.

5.6. Auskunftspflicht und Informationspflicht:

Sie haben die Pflicht, den Betroffenen Auskunft zu erteilen über:

- a) die Tatsache, ob Sie personenbezogene Daten des Betroffenen verarbeiten,
- b) den Verarbeitungszweck,
- b) die Kategorien personenbezogener Daten, die verarbeitet werden,
- c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,
- d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung,
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung

Daraus resultiert Ihre Pflicht: Der Verantwortliche hat den Betroffenen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen.

5.7. Pflicht zur transparenten Information und Kommunikation:

Sie sind verpflichtet, geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung ihrer Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Macht der Betroffene seine o.g. Rechte durch Antrag geltend, haben Sie ihm die Informationen über die ergriffenen Maßnahmen unverzüglich, in jedem Fall aber **innerhalb eines Monats** nach Eingang des Antrags zur Verfügung zu stellen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

5.8. Pflicht zur Erstellung eines Verzeichnisses:

Gemäß Art. 30 der DSGVO müssen Sie ein Verzeichnis (elektronisch oder schriftlich) über alle Verarbeitungstätigkeiten führen. Das heißt für die Praxis: Sie sind verpflichtet, ein Verzeichnis zu erstellen, das folgende Angaben enthält:

- Namen und Kontaktdaten Ihres Unternehmens/ Ihres Vereins etc. und ggf. Ihres Datenschutzbeauftragten
- Ggf. Name und Kontaktdaten desjenigen, in dessen Auftrag die Daten verarbeitet werden
- Zweck der Datenverarbeitung
- Beschreibung der betroffenen Personen (Kunden, Vereinsmitglieder, Beschäftigte etc.)
- Beschreibung der betroffenen Daten (d.h. welche Daten sind betroffen, z.B. Name, Geburtsdatum etc.)
- Empfänger der personenbezogenen Daten (Abnehmer, Behörden ...)
- Ggf. Beschreibung des Drittlandes oder der internationale Organisation, die als Empfänger in Betracht kommt
- wenn möglich, die vorgesehenen Fristen für die Löschung der Daten (z.B. nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist)
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zum Schutz der Daten

6. Welche Rechte hat der Betroffene:

Mit den o.g. datenschutzrechtlichen Pflichten gehen auch einige Rechte des Betroffenen einher, die dieser jederzeit geltend machen kann und die mit den Pflichten korrespondieren. Dazu gehören:

6.1. Auskunftsrecht:

Mit der Auskunftspflicht (siehe 4.6.) korrespondiert das Recht das Betroffenen jederzeit Auskunft über Umfang, Art, Verwendung etc. der über ihn erhobenen Daten zu verlangen. An dieser Stelle sei auf die Ausführungen unter Punkt 4.6. verwiesen.

6.2. Recht auf Berichtigung und Löschung:

Aus der Pflicht zur korrekten Erfassung, Berichtigung und Löschung von Daten (4.2.) ergibt sich das Recht des Betroffenen, jederzeit die Berichtigung oder Löschung seiner personenbezogenen Daten zu verlangen.

6.3. Widerspruchsrecht:

Der Betroffene kann der Verarbeitung seiner Daten jederzeit widersprechen.

7. Bin ich verpflichtet einen Datenschutzbeauftragten zu beschäftigen?

Nicht jeder, der auch personenbezogene Daten verarbeitet, ist verpflichtet, einen Datenschutzbeauftragten zu benennen.

Die Pflicht einen Datenschutzbeauftragten zu benennen, besteht, wenn:

- mindestens 10 Personen (mehr als 9) in dem Betrieb / Unternehmen / Verein etc. mit der automatisierten Datenverarbeitung beschäftigt sind,
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden
- die besonders schutzwürdigen, unter Punkt 3. genannten personenbezogenen Daten verarbeitet werden.

Der Datenschutzbeauftragte muss entsprechend geschult und fachlich geeignet sind. Es besteht auch die Möglichkeit, einen externen Datenschutzbeauftragten zu engagieren.

8. Was passiert, wenn ich gegen die DSGVO verstoße?

Die Datenschutzbehörden der Bundesländer und die Datenschutzbeauftragte des Bundes kontrollieren und überprüfen, ob die datenschutzrechtlichen Bestimmungen eingehalten und umgesetzt wurden.

Durch die neue DSGVO wurden die Rechte und die Macht der Datenschutzbehörden gestärkt.

So sind sie berechtigt Abmahnungen und Verwarnungen auszusprechen, Ortstermine wahrzunehmen und Bußgelder zu verhängen.

Geldbußen:

Die DSGVO sieht vor, dass die Aufsichtsbehörde bei Verstößen gegen das DSGVO Geldbußen bis zu

20.000.000 EUR verhängen kann.

Maßgeblich für die Höhe der Geldbuße sind dabei Art, Schwere und Dauer des Verstoßes und die Tatsache, ob vorsätzlich oder fahrlässig gehandelt wurde. Die Höhe der Geldbuße ist immer eine Frage des Einzelfalls.

Nun müssen Sie nicht befürchten, dass bei jedem Verstoß eine Geldbuße in Millionenhöhe gegen Sie verhängt wird. Der Gesetzgeber wollte den Aufsichtsbehörden mit dieser Befugnis lediglich die Möglichkeit einräumen, auch gegenüber wirtschaftlich sehr starken Konzernen und Unternehmen (wie z.B. google oder facebook) Geldbußen in einer Höhe zu verhängen, die selbst für einen solchen „Wirtschaftsriesen“ finanziell einschneidend sind.

In weniger schweren Fällen wird die Aufsichtsbehörde zunächst eine Verwarnung aussprechen, mit der Aufforderung, den datenschutzwidrigen Zustand innerhalb einer bestimmten Frist auszuräumen.

Wir hoffen, wir konnten Ihnen einen ersten Überblick über die wichtigsten Bestimmungen der DSGVO verschaffen und mögliche Unsicherheiten im Umgang mit den Daten bereinigen. Für weitere Rückfragen stehen wir Ihnen gern zur Verfügung.

*Ihr Team der
Sozietät Kraft & Friederich GbR
Rechtsanwälte und Steuerberater
Tieckstraße 2, 14469 Potsdam*