

# DATENSCHUTZ-GRUNDVERORDNUNG DSGVO

Gültig seit dem 25. Mai 2016



CC-by-sa/3.0 de Detlev Molitor // Business View Photo Ag  
*EU, inkl. Makierung Brexit (nicht EU)*

Die **EU-Datenschutz-Grundverordnung** ist bereits am **25. Mai 2016**, zwanzig Tage nach der Veröffentlichung im EU-Amtsblatt, in Kraft getreten. Nach der darin geregelten **Übergangsfrist** kommt sie allerdings erst zwei Jahre nach Inkrafttreten zur Anwendung. Das bedeutet, dass sie ab **25. Mai 2018 für alle** gilt und deren Einhaltung durch die EU-Datenschutzaufsichtsbehörden und Gerichte überprüfbar ist.

## ***Immer auf der sicheren Seite***

**Sie haben eine Webseite mit Drupal, WordPress, kirby, Redaxo, Joomla, TYPO3, concrete5, Strato, HTML, PHP?**

Der [AGB Hosting-Service](#)<sup>1</sup> (Rechtstext Hosting für Firmen-Webseiten und Blogs) von [janolaw](#)<sup>2</sup> sorgt dafür, dass Ihre AGB und alle weiteren Rechtstexte (Widerrufsbelehrung, Impressum und Datenschutzerklärung) immer den gesetzlichen Anforderungen entsprechen. janolaw garantiert Ihnen dauerhaften Abmahnschutz: Die rechtlichen Texte werden bei gesetzlichen Neuerungen oder geänderter Rechtsprechung bzw. Bedingungen und Richtlinien bei Bedarf automatisch aktualisiert. So entspricht Ihr Internetshop immer den aktuellen Anforderungen.

Durch die Einbindung der Rechtstexte per Schnittstelle können die Anwälte und IT-Spezialisten von janolaw Ihre AGB, Widerrufsbelehrung, Datenschutzerklärung und Impressum immer dann aktualisieren, wenn dies rechtlich erforderlich ist. Bei der Nutzung des AGB Hosting-Service erfolgt die Aktualisierung automatisch ohne dass Sie selbst tätig werden müssen. Die Integration der juristischen Dokumente ist durch die komfortable Schnittstellen-Lösung zu vielen Shopsystemen mit wenigen Handgriffen erledigt.

## **DATENSCHUTZ-GRUNDVERORDNUNG // DSGVO**

# ***Was Unternehmen und Admins jetzt tun müssen***

Ab dem 25. Mai 2018 gilt europaweit ein neues Datenschutz-Gesetz, das für Unternehmen neue rechtliche Verpflichtungen schafft. Trotz der nahenden Frist sind viele IT-Firmen schlecht vorbereitet.

## ***Für mein Business, Geschäft, Praxis, Gaststätte?***

***Ja, denn das neue Monster Datenschutz betrifft jedes Unternehmen, und zwar unabhängig vom Umsatz oder der Anzahl der Beschäftigten.***

- Schon der Empfang von E-Mails, gehört zur Datenverarbeitung und damit zum Datenschutz.
- Datenschutzbeauftragte sind ab 10 Mitarbeiter verpflichtend, kann aber auch darunter gelten, wenn die Daten einer Vorkontrolle unterliegen.
- Datenschutzbeauftragte müssen Fachkunde nachweisen, Zuverlässig ( keine Interessenkonflikte) und müssen sich regelmäßig weiterbilden.
- Der Geschäftsführer kann nicht gleichzeitig Datenschutzbeauftragter sein.
- Verfahrensverzeichnis und Weiterverarbeitungsübersicht für Jedermann anzulegen
- Es muss gewährleistet sein, das bei Änderung der IT eine Anpassung des Verfahrensübersicht erfolgt, ggf. schon bei einem WordPress Update
- Gibt es einen Ablaufplan, für den Fall einer Datenpanne

---

1 <https://business-view.photo/go/13722/>

2 <https://business-view.photo/go/13722/>

## **Was auf Geschäftsführung und Admins zukommt.**

Als im Frühjahr 2016 der finale Text der neuen Datenschutz-Grundverordnung (kurz: DSGVO) veröffentlicht wurde, erntete die EU viel Zuspruch dafür. Die Verordnung sei "eine gute Nachricht für Verbraucher und Unternehmen", zeigten sich die Verbraucherschützer des VZBV (Verbraucherzentrale Bundesverband) überzeugt. Auch die [EU-Kommission](#)<sup>3</sup> war voll des Lobes: Das neue Gesetz markiere einen "wichtigen Meilenstein" und sei "der Höhepunkt" für Europas Datenschutz.

Aber wie sieht es auf Unternehmensseite aus? Was müssen Admins und IT-Verantwortliche beachten, um nach dem 25. Mai weiterhin gesetzeskonform zu arbeiten? Trotz der nahenden Frist für die Einhaltung der neuen Regeln schleift die Umsetzung in der Praxis offenbar noch immer erheblich. "Nur rund jedes achte Unternehmen wird nach eigener Einschätzung bis zum Stichtag die Vorgaben der DSGVO vollständig umgesetzt haben", sagt der deutsche Verband der Digitalwirtschaft [Bitkom](#)<sup>4</sup>. Und einer Umfrage des IT-Sicherheitsunternehmens [Watchguard](#)<sup>5</sup> zufolge wissen fast die Hälfte von 277 befragten Unternehmen in Deutschland noch nicht einmal, ob die DSGVO für sie überhaupt greift .

Grund genug, die wichtigsten Neuerungen und Verpflichtungen für Unternehmen und Admins genau zu untersuchen. Denn wer den neuen Verpflichtungen nach dem 25. Mai nicht nachkommt, riskiert hohe Bußgelder. Auch wenn die häufig zitierten Maximalstrafen von 20 Millionen Euro beziehungsweise 4 Prozent des globalen Unternehmensumsatzes in der Praxis eher die Ausnahme bleiben dürften, können Bußgelder in Abhängigkeit der Schwere des Vorfalls und der Unternehmensgröße schnell an die Substanz gehen.

## **Was sind personenbezogene Daten?**

Die DSGVO regelt, wie Unternehmen mit personenbezogenen Daten umgehen müssen. Die Verordnung fasst den Begriff der personenbezogenen Daten sehr weit. Beispiele für personenbezogene Daten nach DSGVO sind laut EU-Kommission neben Name, Anschrift und E-Mail-Adresse auch Ausweisnummer, Standortdaten, IP-Adressen, Cookie-Kennungen, Werbe-IDs und Gesundheitsdaten aus Krankenhäusern oder bei Ärzten, die zur eindeutigen Identifizierung einer Person führen könnten.

Grundsätzlich gelten alle Informationen als personenbezogen, die sich auf eine "identifizierte oder identifizierbare lebende Person" beziehen. Identifizierbar bedeutet, dass selbst wenn es auch nur theoretisch möglich ist, durch die Kombination verschiedener Teilinformationen bestimmte Personen zu identifizieren, diese Teilinformationen bereits ebenfalls personenbezogene Daten darstellen.

Dies betrifft Informationen der EU-Kommission zufolge auch personenbezogene Daten, die anonymisiert, verschlüsselt oder pseudonymisiert wurden, aber zur erneuten Identifizierung einer Person genutzt werden könnten. Erst wenn die Daten so anonymisiert wurden, dass auch mit größerem Aufwand keine Rückschlüsse mehr auf die betroffenen Personen gezogen werden können, gelten Daten als nicht mehr personenbezogen.

Wie schwer eine rechtssichere Anonymisierung großer Datenmengen ist, demonstrierte [Netflix](#)<sup>6</sup> unfreiwillig schon vor über zehn Jahren. Die von dem Unternehmen veröffentlichten anonymisierten Filmbewertungen von rund einer halbe Million Kunden konnten von Forschern direkt mit öffentlichen Ratings der Internet Movie Database IMDb korreliert und ein Teil der

---

3 [http://europa.eu/rapid/press-release\\_STATEMENT-16-1403\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm)

4 <https://www.bitkom.org/Presse/Presseinformation/Datenschutzgrundverordnung-Jeder-Zweite-holt-sich-Hilfe.html>

5 <https://www.channelpartner.de/a/47-prozent-der-unternehmen-blank,3332933>

6 <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt>

Datensätze so Personen zugeordnet werden.

Ähnlich erging es vor einigen Jahren einem rund 20 GByte großen, eigentlich pseudonymisierten Datensatz mit Informationen über 170 Millionen [Taxifahrten](#)<sup>7</sup> in New York. Wegen Fehlern beim Hashen sowie mit Hilfe zuvor bekannter Eigenschaften der pseudonymisierten Daten war die anschließende Deanonymisierung der betroffenen Taxis ein Kinderspiel. Auch deswegen verlangt die DSGVO, dass die Anonymisierung unumkehrbar sein muss, damit die Daten ihre rechtliche Eigenschaft der Personenbezogenheit verlieren.

Technische Vorgaben dazu, wie eine rechtssichere Anonymisierung oder Pseudonymisierung gelingen kann, enthält die DSGVO nicht. "Es gibt im Prinzip zwei Möglichkeiten", erklärt Rechtsanwalt Martin Schirmbacher im Gespräch mit [Golem.de](#)<sup>8</sup>. "Entweder man entfernt identifizierende Merkmale wie etwa Namen oder Geburtsdaten oder man aggregiert die Daten so, dass man den Rückschluss auf eine Person nicht mehr ziehen kann." In jedem Fall empfiehlt Schirmbacher Unternehmen, die jeweils gewählte Anonymisierungstechnik ausgiebig zu dokumentieren. "Wie überall in der DSGVO ist eine transparente Dokumentation hier essenziell."

## **Keine Datenverarbeitung ohne Rechtsgrundlage**

Grundsätzlich gilt in der DSGVO das sogenannte "*Verbot mit Erlaubnisvorbehalt*". Das heißt, jede Verarbeitung personenbezogener Daten ist verboten, es sei denn ein Gesetz erlaubt sie explizit. Es muss also stets eine Rechtsgrundlage her, von denen die DSGVO aber glücklicherweise bereits fünf bereithält. Die Frage, welche Rechtsgrundlage sich für welchen Anwendungszweck am besten eignet, ist heute noch schwer abschließend zu klären. Die Antwort hängt von der Art der Datenverarbeitung und insbesondere von der zukünftigen Rechtsprechung zur DSGVO ab.

Personenbezogene Daten dürfen grundsätzlich verarbeitet werden, wenn dies zur Erfüllung eines Vertrages oder aufgrund gesetzlicher Verpflichtungen notwendig ist. Dazu gehören beispielsweise Bestell- und Adressdaten von Kunden eines Onlineshops oder Daten, die aufgrund steuerrechtlicher Archivierungspflichten aufbewahrt werden müssen.

Weiterhin ist eine Datenverarbeitung wie bisher auch aufgrund eines "berechtigten Interesses" möglich. "Hierunter fallen nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen, die von der Rechtsordnung [anerkannt werden](#)<sup>9</sup>", schreibt der Rechtsanwalt Henry Pohling. Dabei müsse ein solches berechtigtes Interesse in Zukunft aber von Fall zu Fall gegen "die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern", abgewogen werden.

Wie diese rechtliche Abwägung genau ausgestaltet werden wird, ist derzeit noch nicht vollständig absehbar. Pohling zufolge müssen die schutzwürdigen Interessen der Betroffenen die Interessen des Datenverarbeiters aber überwiegen, damit eine Datenverarbeitung unzulässig ist. Für eine Datenverarbeitung wie beim E-Mail-Marketing komme man aber mit dem berechtigten Interesse nicht weit, sagt Rechtsanwalt Schirmbacher. Handele es sich bei den Empfängern nicht ausschließlich um Bestandskunden, denen man das bereits erworbene Produkt noch einmal anbieten möchte, brauche es die Einwilligung der Betroffenen. Aber auch die hat in der DSGVO ihre Tücken.

## **Komplizierte Einwilligung**

Personenbezogene Daten dürfen natürlich weiterhin auch dann verarbeitet werden, wenn dafür die

7 <https://www.golem.de/news/hashfunktionen-datenbank-ueber-new-yorker-taxis-deanonymisiert-1406-107459.html>

8 <https://www.golem.de/news/datenschutz-grundverordnung-was-unternehmen-und-admins-jetzt-tun-muessen-1803-133122.html>

9 <https://www.pingdigital.de/blog/2017/08/21/berechtigte-interessen-nach-der-dsgvo/1186>

Einwilligung der Betroffenen vorliegt. Diese ist jedoch unter den neuen Regeln der DSGVO viel schwerer zu bekommen, muss aufwendig belegt sein und kann jederzeit widerrufen werden. Zwar ist es nicht mehr nötig, eine Einwilligung per Schriftform einzuholen, eine digitale Einwilligung ist jedoch im Streitfall auch schwerer zu belegen. Sie sollte idealerweise in einer Datenbank einschließlich Datums- und Zeitangabe protokolliert sein. Technisch eignet sich dafür wie bisher auch ein per E-Mail versandter Bestätigungslink, auf den Nutzer klicken müssen, um so ihre explizite Einwilligung zur Datenverarbeitung mitzuteilen.

"Der Nachweis der Einwilligung muss konkret erfolgen", sagt Rechtsanwalt Schirmbacher. "Da reicht es nicht zu sagen, man hole ja immer Einwilligungen ein. Ich muss nachweisen können, dass jemand, der sich beispielsweise für einen Newsletter eingetragen hat, diesen Text angezeigt bekommen hat. Und wer seine E-Mail-Adresse eingetragen hat, hat auch eine Bestätigungsmail bekommen." Es sei zudem ratsam, die Bestätigungsmail einschließlich Datums- und Zeitstempel des Klicks auf den Bestätigungslink sowie die IP-Adresse der Betroffenen in einem ausdrückbaren Format zu speichern, um die Einwilligung gegebenenfalls beweisen zu können.

### **Informiert und freiwillig zustimmen**

Darüber hinaus muss eine Einwilligung in informierter Weise unmissverständlich in Form einer Erklärung oder einer sonstigen eindeutigen Handlung abgegeben werden. Das soll eine bloße implizite Zustimmung zum Beispiel durch das Nichtwegklicken eines vorausgewählten Häkchens oder einen anderen fehlenden Widerspruch (Opt-out) ausschließen. Entscheidend ist laut DSGVO eine eindeutige Handlung der Betroffenen.

Komplex ist die Einwilligung zudem, weil sie vollkommen freiwillig abgegeben werden muss. In der Praxis wird eine Freiwilligkeit wohl nur als gegeben gelten, wenn sich die Betroffenen in keiner Weise gedrängt oder gezwungen fühlen, eine Einwilligung abzugeben. Nur wer ohne Konsequenzen auch nein sagen kann, hat demnach wirklich freiwillig zugestimmt. In der Bewertung der Freiwilligkeit kann auch ein zum Beispiel in Onlineshops künstlich suggerierter Zeit- oder Knappheitsdruck eine Rolle spielen.

Auch wenn einige Kommentatoren ein absolutes [Kopplungsverbot](#)<sup>10</sup> verneinen, scheint der Gesetzgeber doch verhindern zu wollen, dass Nutzer allzu leichtfertig in den Deal "kostenlose Dienste gegen persönliche Daten" einwilligen. Ein Anbieter eines kostenlosen E-Mail-Postfachs sollte jedenfalls in Zukunft gut argumentieren, wenn er Nutzer von seinem Angebot ausschließen will, weil diese der Verarbeitung ihrer Daten zu Werbezwecken nicht zustimmen wollen.

### **Dokumentations-, Nachweis- und Rechenschaftspflichten**

Die neuen Verpflichtungen der DSGVO erschöpfen sich jedoch nicht in der Feststellung einer Rechtsgrundlage. Über das Dokumentieren von Einwilligungen hinaus müssen Unternehmen mit 250 oder mehr Mitarbeitern ein umfangreiches Verzeichnis aller dort stattfindenden Datenverarbeitungsvorgänge führen. Unter bestimmten Voraussetzungen kann diese Pflicht sogar für kleinere Unternehmen gelten.

Zwar macht die Verordnung keine Vorgaben dazu, wie ein solches Verzeichnis auszusehen hat, es ist aber ratsam, dieses im Zweifel eher zu detailliert zu führen. Zu jedem Datenverarbeitungsvorgang sollte festgehalten werden, auf welcher Rechtsgrundlage er durchgeführt wird, welche Art personenbezogener Daten zu welchem Zweck verarbeitet werden, auf welche Art und Weise sie gesammelt wurden und wie lange sie aufbewahrt werden. Die deutschen

---

<sup>10</sup> <https://www.pingdigital.de/blog/2017/08/17/bedeutet-das-kopplungsverbot-nach-der-dsgvo-das-aus-fuer-einwilligungen/1167>

Landesdatenschutzbehörden stellen ein [Musterverzeichnis über Verarbeitungstätigkeiten](#)<sup>11</sup> gemäß DSGVO zum Download zur Verfügung, an dem sich Unternehmen orientieren können. Selbst in überschaubar großen Unternehmen mit einer limitierten Anzahl vorhandener Datenverarbeitungsvorgänge wird deutlich, dass ein solches Verzeichnis schnell beachtliche Ausmaße annehmen kann. Wer jetzt erst mit dessen Erstellung beginnt, ist bereits spät dran.

**Hinweis:** Nicht alle Unternehmen werden bisher jeder Datenverarbeitung eine bestimmte Rechtsgrundlage zugeordnet haben. Unter der DSGVO muss das Unternehmen neuerdings den Betroffenen in der Datenschutzerklärung darüber informieren, auf welche Rechtsgrundlage man die Datenverarbeitung stützt (Permanente Auskunftspflicht S. 7). Falls dies unter Art. 6 Abs. 1 lit. f DSGVO erfolgt, müssen auch die berechtigten Interessen des Verantwortlichen aufgeführt werden. Sie sollten daher die Rechtsgrundlagen in Zusammenhang mit den unterschiedlichen Datenverarbeitungen dokumentieren. So können Sie auch schneller bei Auskunftsansprüchen von Betroffenen, Anfragen von Aufsichtsbehörden etc. reagieren. Behalten Sie auch im Kopf, dass an verschiedene Rechtsgrundlagen unterschiedliche Rechte geknüpft sind. So kann die Einwilligung z. B. jederzeit widerrufen werden, wohingegen ein Widerspruch nur unter bestimmten Voraussetzungen erfolgen kann. Sie sollten sich also schon bei der Erhebung der Daten darüber Gedanken machen, welche Rechtsgrundlage für die jeweilige Datenverarbeitung geeignet ist.

## **Weitergabe personenbezogener Daten und Outsourcing der Verarbeitung an Dritte**

Insbesondere für IT-Unternehmen, Plattform- und App-Anbieter hält die DSGVO noch eine weitere Herausforderung bereit. Sobald personenbezogene Daten an Dritte zur Verarbeitung weitergegeben werden - sogenannte Auftragsverarbeitung -, sollte ein Auftragsverarbeitungsvertrag her. Dieser regelt die Rechte und Pflichten des Auftragsverarbeiters und bestätigt, dass dieser ebenfalls DSGVO-konform arbeitet, wozu unter anderem wiederum ein eigenes Verzeichnis der Datenverarbeitungsvorgänge zählt.

**Achtung:** Schon das einfache Speichern personenbezogener Daten in einem S3-Bucket von Amazon oder in einer Dropbox gilt als Auftragsverarbeitung. "Bereits die Möglichkeit eines Zugriffs zum Beispiel durch einen Hostler reicht, damit man eine Datenverarbeitung annehmen kann", erklärt Martin Schirnbacher. "Wenn die Daten nicht verschlüsselt sind, fallen sie unter die Auftragsverarbeitung." Weitere Beispiele für eine Auftragsverarbeitung sind die Verwaltung von Kundendaten auf einer **extern gehosteten CRM-Plattform**, das Speichern von E-Mail-Adressen bei Mailchimp oder der Einsatz eines externen Projektmanagement-Dienstes wie Podio.

"Das ist an sich keine Katastrophe", sagt Schirnbacher. Auftragsverarbeiter müssten eben eine Vereinbarung anbieten, die die Kunden mit ihnen schließen können. Unternehmen, die personenbezogene Daten verarbeiten, sollten also bei der Auswahl ihres Cloud-Anbieters darauf achten, sich abzusichern. Auch hier gilt laut Schirnbacher: "Ich muss den Dienstleister ordentlich auswählen. Das heißt, ich muss mich selbst davon überzeugen, dass es technische und organisatorische Maßnahmen zum Schutz der Daten gibt und dass nicht jeder Praktikant in die Daten reinschauen kann."

Darunter könnten in Zukunft möglicherweise kleinere Cloud-Anbieter leiden, wenn es ihnen nicht

---

<sup>11</sup> [https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeichnis\\_und\\_verfahrensregister\\_nach\\_bds/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html](https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeichnis_und_verfahrensregister_nach_bds/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html)



gelingt, ihre Kunden von der Rechtssicherheit der Datenverarbeitung auf ihren Systemen zu überzeugen. Um den Prozess zu vereinfachen, bietet die niedersächsische Landesdatenschutzbeauftragte ein [Muster für einen DSGVO-konformen Auftragsverarbeitungsvertrag](#)<sup>12</sup> auf ihrer Webseite zum Download an.

## **Permanente Auskunftspflicht**

Über das sogenannte "Recht auf Vergessenwerden" in der EU wurde viel [geschrieben](#)<sup>13</sup> und noch mehr [gestritten](#)<sup>14</sup>. Die DSGVO gestaltet dieses Recht nun aus und kombiniert es mit einer Reihe weitreichender Pflichten für Verarbeiter personenbezogener Daten. Diese müssen zukünftig auf Anfrage einer Person nicht nur jederzeit Auskunft darüber geben, ob sie personenbezogene Daten über diese Person verarbeiten oder nicht. Unternehmen sind außerdem verpflichtet, auf Anfrage eine Kopie solcher personenbezogenen Daten zur Verfügung zu stellen.

Werden die betreffenden Daten auf elektronischem Wege verarbeitet, müssen solche Auskunftersuchen auch auf elektronischem Weg gestellt werden können. Eine Postanschrift alleine ist in solchen Fällen also unzulässig. Insbesondere Unternehmen, die personenbezogene Daten einer großen Anzahl von Einzelpersonen verarbeiten, wie es bei den meisten Onlinediensten heute der Fall ist, sollten sich auf solche Anfragen technisch gut vorbereiten. Denn die DSGVO verpflichtet Datenverarbeiter, solche Anfragen "unverzüglich" zu beantworten, laut [EU-Kommission](#)<sup>15</sup> grundsätzlich "spätestens innerhalb eines Monats nach Eingang des Antrags".

Einer repräsentativen [Verbraucherumfrage](#)<sup>16</sup> zufolge geben zudem 55 Prozent der Befragten an, ihre eigenen Daten einsehen zu wollen und 59 Prozent sagen, sie hätten Interesse daran, Informationen löschen zu lassen. Für Entwickler ist es also ratsam, in ihrer Software bereits jetzt automatisierte Möglichkeiten für den individuellen Datenexport auf Anfrage von Nutzern vorzusehen. Liegen die ersten Auskunftersuchen erst einmal auf dem Tisch, ist es für eine Umstellung möglicherweise zu spät.

## **Datenschutz "by Design" und "by Default"**

Und noch einen weiteren Punkt sollten Produktentwickler und Programmierer berücksichtigen: Die DSGVO enthält erstmals die verpflichtenden Prinzipien des Datenschutzes durch Technikgestaltung ("by Design") und durch datenschutzfreundliche Voreinstellungen ("by Default"). Bei Ersterem handelt es sich um die Verpflichtung, bei der Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen zu treffen, um diese angemessen zu schützen.

Das kann laut DSGVO beispielsweise dadurch erreicht werden, dass die Verarbeitung personenbezogener Daten von Anfang an minimiert und solche Daten im System so schnell wie möglich pseudonymisiert werden. Außerdem sollten Entwickler unter Berücksichtigung des Stands der Technik entsprechende technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten zu schützen. Das könnte beispielsweise neue Messenger-Apps ohne zumindest eine Transportverschlüsselung in Zukunft ausschließen.

---

12 <https://www.lfd.niedersachsen.de/download/127630>

13 <https://www.golem.de/news/recht-auf-vergessenwerden-google-sperrt-links-fuer-alle-europaeischen-nutzer-1602-119020.html>

14 <https://www.golem.de/news/recht-auf-vergessenwerden-eugh-entscheidet-ueber-weltweite-auslistung-von-links-1707-129044.html>

15 [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/how-do-we-deal-requests-individuals-exercising-their-data-protection-rights\\_de](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/how-do-we-deal-requests-individuals-exercising-their-data-protection-rights_de)

16 <https://www.pressebox.de/inaktiv/hubspot-inc/Neue-Studie-EU-DSGVO-trifft-Marketing-unvorbereitet/boxid/881281>

Das Prinzip des Datenschutzes by Default dagegen verpflichtet Entwickler, Standardeinstellungen in ihren Produkten und Programmen so zu setzen, dass "durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden", wie es in der DSGVO heißt. Bietet ein Browser beispielsweise an, Cross-Site-Tracking zu blockieren oder Cookies von Drittanbietern abzulehnen, müssten solche Optionen in Zukunft standardmäßig eingeschaltet sein, wenn die damit gesammelten Daten nicht für die Funktion des Browsers notwendig sind.

### ***take it or leave it***

Art. 7 Abs. 4 DSGVO in Verbindung mit Erwägungsgrund 34 untersagt, dass der Abschluss eines Vertrags von der Erteilung einer Einwilligung abhängig gemacht wird, obwohl dies für die Durchführung des Vertrags nicht erforderlich ist (kein »take it or leave it«). Damit dehnt die DSGVO die bestehende Regelung des § 28 Abs. 3b BDSG in Monopolsituationen deutlich aus. In der Praxis könnte diese bedeuten, dass Unternehmen ihre Dienstleistung einmal mit und einmal ohne Einwilligung anbieten müssen.

### ***Neue Datenschutzerklärung***

Wie bisher auch werden Unternehmen, die personenbezogene Daten verarbeiten, in der DSGVO dazu verpflichtet, Betroffene darüber in einer Datenschutzerklärung zu informieren. Neu sind die hohen Anforderungen, denen eine Datenschutzerklärung genügen muss: Alle Informationen müssen **"leicht zugänglich, verständlich und in klarer und einfacher Sprache"** abgefasst sein und **"gegebenenfalls zusätzlich visuelle Elemente"** enthalten, heißt es in der Verordnung. Angesichts der Menge an Informationen, die eine Datenschutzerklärung zukünftig mindestens enthalten muss, ist das alleine bereits eine enorme Herausforderung.

Informiert werden müssen Betroffene unter anderem über ihr Recht auf Auskunft bezüglich der über sie verarbeiteten Daten, ihr Recht auf Berichtigung derselben, ihr Recht auf Widerspruch gegen die Verarbeitung sowie ihre Rechte auf Vergessenwerden und auf Datenübertragbarkeit. Darüber hinaus müssen Betroffene natürlich über den Zweck und die Rechtsgrundlage der Datenverarbeitung aufgeklärt werden.

Als ob dies nicht schon schwierig genug wäre, müssen solche Informationen, wenn es sich zum personenbezogene Daten von Kindern handelt, aufgrund deren besonderer Schutzwürdigkeit so formuliert sein, dass sie auch von Kindern verstanden werden. Möglicherweise entwickelt sich wegen der DSGVO ein ganz neuer Berufszweig für "Datenschutzerklärungsformulierer" als eine Schnittmenge aus Juristinnen, Erziehern und Sprachwissenschaftlerinnen.

### ***Fazit***

Die neue DSGVO wird ab dem 25. Mai 2018 europaweit weitgehend einheitliche, insgesamt strengere Datenschutzregeln etablieren. Diese werden jedes Unternehmen und jede Organisation betreffen, die in irgendeiner Form personenbezogene Daten verarbeiten. Auch wenn die Rechtsgrundlagen, aufgrund derer eine solche Datenverarbeitung zulässig ist, viel Raum für verschiedene Verarbeitungszwecke lassen, sind die Anforderungen an die Verarbeiter erheblich gestiegen.

Die neuen Dokumentations-, Nachweis- und Rechenschaftspflichten, die Auskunftspflichten gegenüber Betroffenen und erst recht die Herkulesaufgabe einer DSGVO-konformen Datenschutzerklärung sollte jedes Unternehmen schnellstens in Angriff nehmen. Dazu gehört



mindestens die [Lektüre des Rechtstextes](#)<sup>17</sup> selbst beziehungsweise eines juristischen Ratgebers. Für die meisten Unternehmen empfiehlt sich außerdem die Hinzuziehung interner oder externer Rechtsberatung.

Bei der Vorbereitung auf die neue Rechtslage sollten neben der Geschäftsleitung und der Datenschutzbeauftragten auch die für die Umsetzung zuständigen Admins miteinbezogen werden. Zwar haftet bei Verstößen zuerst einmal das Unternehmen beziehungsweise die Unternehmensleitung, nicht der Sysadmin. Eine korrekte Umsetzung der Anforderungen der DSGVO ist aber ohne die Einbeziehung und Schulung der verantwortlichen Mitarbeiter nur schwer zu machen.

Die hohen potenziellen Strafen für eine Nichteinhaltung der neuen Regeln machen den Versuch, irgendwie unbemerkt unter dem Radar durchzufliegen, für Unternehmen zu einem riskanten Unterfangen. Verstöße gegen die Grundsätze und die Regeln betreffend die Rechtmäßigkeit der Verarbeitung sind mit Geldbußen bis zu EUR 20 Mio oder im Falle eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bedroht.

## **Was ist zu tun? - Die Bürokratie des Grauens!**

- Von Microsoft Deutschland gibt es einen Test, 9 Fragen um zu wissen wo Sie stehen [DSGVO-Check](#)<sup>18</sup>
- Das Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) hat eine [DSGVO – Selbsteinschätzung](#)<sup>19</sup>, bei dem man sich spielerisch auf eine Reise durch Datenschutz-Europa begeben kann.
- Und so langsam wird es ernst, mit dem [Fragebogen zur Umsetzung](#)<sup>20</sup> der DSGVO zum 25. Mai 2018, als PDF Datei.

## **Was ist neu? Was muss beachtet werden?**

**Unterrichtungspflicht:** Kunden, vor allem Neukunden, muss Folgendes klar dargestellt werden:

- Wofür werden Ihre Daten verwendet?
- Wo und wie lange werden Sie gespeichert?
- An wen werden Sie übermittelt? (vor allem bei Leistungsträgern / Lieferanten außerhalb der EU)
- Wie kann der Kunde seine Daten erhalten, berichtigen, einschränken oder löschen lassen?
- Daten müssen Freiwillig gegeben werden! Die Erteilung der Einwilligung erfordert eine freiwillige, spezifisch informierte und eindeutige Handlung – z. B. das Anklicken eines Kästchens auf einer Webseite und die Auswahl technischer Einstellungen bei Online-Diensten. Keine Einwilligung stellen laut Erwägungsgrund 32 zur DSGVO ein stillschweigendes Einverständnis, standardmäßig angekreuzte Kästchen oder Untätigkeit des Betroffenen dar.
  - Zudem fordert die DSGVO, dass in verschiedene Datenverarbeitungsvorgänge jeweils

---

17 <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE>

18 <https://www.microsoft.com/de-de/aktion/IT-Sicherheit/dsgvo-check-wizard.aspx>

19 <https://www.lda.bayern.de/tool/start.html>

20 [https://business-view.photo/wp-content/uploads/2017/12/dsgvo\\_fragebogen.pdf](https://business-view.photo/wp-content/uploads/2017/12/dsgvo_fragebogen.pdf)

gesondert eingewilligt werden muss. Andernfalls soll es an der Freiwilligkeit fehlen.

- Der Betroffene muss seine Einwilligung jederzeit und ohne Begründung widerrufen können. Der Widerruf der Einwilligung ist mindestens so einfach zu gestalten wie die Abgabe (Art. 7).

**Hinweis:** Nach der DSGVO müssen Sie den Nachweis erbringen, dass eine effektive Einwilligung gegeben wurde. Die Einwilligung kann auch elektronisch abgegeben werden.

**Zweckbindung, Datenminimierung und Transparenz:** Zwar bleiben die allgemeinen Grundsätze gleich, allerdings werden diese in strengeren Vorschriften konkret umgesetzt, z. B. bei der Weiterverarbeitung von Daten gem. Art. 6 Abs. 4 DSGVO (Zweckbindung), durch die Verpflichtung zu Privacy by Design (S. 7) und datenschutzrechtlichen Voreinstellungen gem. Art. 25 DSGVO (Datenminimierung) und den zusätzlichen Informationspflichten in Art. 13 und 14 DSGVO (Transparenz).

**Hinweis:** Für die Verarbeitung von sensiblen Daten gelten die in Art. 9 DSGVO<sup>21</sup> aufgeführten Voraussetzungen (explizite Einwilligung).

**Dokumentations- und Nachweispflicht:** Alle personenbezogenen Datenverarbeitungstätigkeiten müssen im Betrieb sorgfältig dokumentiert werden und jederzeit auf Verlangen der Datenschutzbehörde vorgelegt werden. Die DSGVO gibt vor, dass Daten nur verarbeitet werden dürfen, wenn auch eine rechtliche Grundlage besteht, beziehungsweise das Unternehmen die Einwilligung der betroffenen Person hat. Unternehmen werden nun beweispflichtig, dass die Daten rechtmäßig verarbeitet werden.

**Check:** Sie sollten dokumentieren welche personenbezogenen Daten Ihr Unternehmen verarbeitet, woher Sie diese Daten haben und an wen Sie die Daten weitergegeben. Andernfalls wird es schwierig dieser Vorgabe der DSGVO nachzukommen. Sie sollten zusätzlich Ihr Lösungsverfahren im Unternehmen prüfen, sodass bei einem Löschanspruch die Daten schnell auffindbar sind und gelöscht werden können. **Name, E-Mail, Geburtsdaten, Adresse, SteuerNummer, Konto, Freizeitgestaltung, Glaubensgemeinschaft, Gewerkschaft, Krankengeschichte...**

**Verfahrensverzeichnis:** Welche Mitarbeiter, externe Dienstleister / Erfüllungsgehilfen und so weiter haben in welchem Umfang Zugriff auf die Daten? In welcher Verbindung stehen Sie zueinander?

**Pflicht zur Selbstanzeige:** Hackerangriffe auf den Daten Server / Computer müssen sofort der zuständigen [Landesdatenschutzbehörde](#)<sup>22</sup> gemeldet werden.

**Daten außer der EU:** Wer Daten außerhalb der EU übermittelt, muss sicherstellen, dass die Informationen dort nach dem Standard der EU-DSGVO behandelt werden. Bei Verstößen des Dienstleisters kann man selbst in Haftung genommen werden!

**Frage:** (1) Ein Google Local Guide, nimmt Änderungen an einem Bestehenden Unternehmen vor, oder legt dieses an? Die Daten werden an Google übermittelt, (Name, Telefonnummer etc.). (2) Ein Dienstleister erstellt ein Facebook Profil, oder Postet News im Auftrag.

**Datenschutz durch Technikgestaltung:** Neue Produkte (Hardware & Software) müssen bereits in

<sup>21</sup> Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

<sup>22</sup> [https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden\\_und\\_Landesdatenschutzbeauftragte](https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte)

der Gestaltung den Prinzipien des Datenschutzes folgen. So muss zum Beispiel Software per Voreinstellung datenschutzfreundlich sein.

**Subunternehmer:** Auch Subunternehmer wie beispielweise Mailing-Dienste, müssen nach den neuen Richtlinien arbeiten, dieses muss bei Erteilung des Auftrages durch den Auftraggeber überprüft werden. Aus Art. 4 Abs. 7 DSGVO ergibt sich zunächst, dass neben der alleinigen Verantwortung auch ein arbeitsteiliges Zusammenwirken möglich ist. Ohne ein solches Zusammenarbeiten kommen selbst kleinere und mittlere Unternehmen heute nur noch selten aus, denn es ermöglicht die Inanspruchnahme besonderer Kenntnisse und Erfahrungen und vermeidet unverhältnismäßige Investitionen. Dabei ist das Zusammenwirken nicht zahlenmäßig beschränkt: Art. 26 DSGVO, die Kernbestimmung über gemeinsam Verantwortliche, nennt zwei oder mehr Verantwortliche und verzichtet damit sinnvollerweise auf eine Obergrenze. Von der gemeinsamen Verantwortung zu unterscheiden ist einerseits die alleinige Verantwortung einer Stelle, die die Entscheidungen über Zwecke und Mittel der Verarbeitung selbst und unabhängig von anderen Stellen trifft, und andererseits die Auftragsverarbeitung.

**Recht auf Vergessen werden:** Da gibt es zwar schon länger, nun wird es verschärft! Die Fristen zum Löschen personenbezogener Daten müssen unbedingt eingehalten werden, am besten durch eine Automatik im System (Datenbank, CRM, Buchhaltung etc.)

***Hinweis:** Steuerunterlagen bis zu 10 Jahre aufbewahren - Aufbewahrungsfrist beginnt mit Schluss des Kalenderjahres. Geschäftsbriefe (E-Mails) – 7 Jahre ...*

**Informationspflichten gegenüber Betroffenen (Kunden & Lieferanten):** Im Besonderen das Recht auf Datenportabilität. Unternehmen müssen betroffenen Personen ihre Daten in einem maschinenlesbaren, gängigen Format aushändigen können, um Kunden so den Weg zu einem anderen Unternehmen zu erleichtern.

***Check:** Sie sollten ab Mai 2018 in der Lage sein auf Anfrage personenbezogene Daten, die der Betroffene selbst bereitgestellt hat, in einem gängigen und elektronischen Format dem Betroffenen bereitzustellen.*

**Verbandsklage:** Mit dem am 17. Februar 2016 erlassenen Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts hat Deutschland bereits die in Art. 80 Abs. 2 DSGVO aufgeführte Öffnungsklausel genutzt. Das neue Gesetz räumt einer Vielzahl an Verbänden z. B. Verbraucherschutzorganisationen ein Klagerecht zur ‚abstrakten Durchsetzung‘, also ohne dass der Betroffene sich selbst beschwert, datenschutzrechtlicher Vorschriften ein. Bisher konnten Verbraucherschützer schon gegen Unternehmen vorgehen, wenn diese in den Allgemeinen Geschäftsbedingungen (AGB) gegen Datenschutzvorschriften verstießen. Diese Befugnis wird nun auch auf andere Vorschriften erweitert, nämlich dann, wenn Daten für Werbung, Markt- und Meinungsforschung, Auskunfteien, Profilbildung, Adresshandel oder vergleichbare kommerzielle Zwecke genutzt werden. In anderen Ländern, die kein Gesetz unter dieser Öffnungsklausel erlassen haben, können Verbraucherschutzverbände nur im Namen eines Betroffenen aktiv werden, wenn sie ein Mandat von ihm erhalten und in seinem Namen tätig werden.

***Hinweis:** Sie sollten in Zukunft in Deutschland also damit rechnen, dass auch Verbraucherschutzverbände Lösch-, Auskunfts- und Schadensersatzansprüche Betroffener einklagen können.*

**Internationale Unternehmen:** Die DSGVO hält für international tätige Unternehmen die gleichen Rechtsinstrumente zur Datenübermittlung in Drittstaaten wie schon die DS-RL bereit (u. a. Einwilligung, Vertrag, Standardvertragsklauseln, Binding Corporate Rules – und sogar noch weitere (Zertifizierung, Codes of Conduct). Zukünftig kann deutschen Unternehmen auch das im Juli 2016

angenommene [Privacy Shield](#)<sup>23</sup> als Rechtsgrundlage dienen, um an US-amerikanische Unternehmen, die sich dazu verpflichtet haben die Datenschutzgrundsätze in dem neuen Instrument einzuhalten, Daten zu übermitteln.

**Hinweis:** Prüfen Sie immer erst, ob die EU-Kommission eine [Angemessenheitsentscheidung](#)<sup>24</sup> für das jeweilige Land, in das Ihr Unternehmen Daten übermittelt, erlassen hat. Liegt eine solche Entscheidung nicht vor, müssen Sie den Datentransfer auf eines der in der Verordnung vorgesehenen Rechtsinstrumente stützen und den Betroffenen hierüber in der Datenschutzerklärung informieren.

## Datenschutzbeauftragte (DSB)

Eine solche Person muss jedes Unternehmen mit mindestens zehn Mitarbeitern benennen. Zu den beschäftigten zählen zum Beispiel Inhaber, Mitarbeiter, und alle Personen die evtl. mit Kunden- oder Mitarbeiterdaten in Kontakt kommen könnten. Im Zweifelsfall also auch das externe Reinigungspersonal, das die Mülleimer leert, oder der Hausmeister der die Lampe repariert.

**CHECK:** Ein kleines Unternehmen bzw. Start-up mit weniger als 9 Angestellten sollte prüfen, ob es in die von Art. 37 Abs. 1 DSGVO genannten Kategorien fällt und einen Datenschutzbeauftragten benötigt!

Sind Sie ein kleines Unternehmen bzw. Start-up mit weniger als 9 Angestellten, sollten Sie prüfen, ob die Tätigkeit Ihres Unternehmens in die oben genannten Kategorien fällt. Falls ja, benötigen Sie trotz Schwellenwert einen betrieblichen Datenschutzbeauftragten. Konzerne können neuerdings auch nur einen DSB für die ganze Unternehmensgruppe (Konzern-Datenschutzbeauftragter) bestimmen, sofern dieser für jede Gesellschaft der Gruppe aus leicht erreichbar ist. Mehrfachbestellungen entfallen damit.

**Aktuell zum Beispiel, prüft die Datenschutz Aufsichtsbehörde Niedersachsen ob Reisebüros nicht grundsätzlich einen DSB benötigen, da diese ständig Daten an Dritte übermitteln. (Veranstalter, Hotels, Airlines usw.)**

Der DSB kann ein Mitarbeiter oder ein externer Dienstleister sein.

## Datenpanne? Was nun?

Es wird teuer, oder sehr teuer! Verletzungen gegen die EU-DSGVO können mit einer Strafe bis zu 4% des Jahresumsatzes geahndet werden. Die Strafe fällt allerdings deutlich Milder aus, wenn man eine Selbstanzeige macht.

Wichtig: Im Zweifelsfall muss nicht der Kunde nachweisen, das mit seinen Daten nicht sorgfältig Umgangen wurde, sondern der Unternehmer, dass er datenschutzkonform gearbeitet hat!

**Wurde ich gehackt? Jetzt den Selbst-Check machen!**

### Have I Been Pwned

Immer wieder kommt es vor, dass Hacker Datenbanken von Unternehmen knacken und Zugangsdaten von Nutzer entwenden. Oft wissen User nicht, ob auch Ihr Account vom Angriff betroffen ist. Auf diese Frage weiß „Have I Been Pwned“ die Antwort.

[.:-have i been pwned?](#)<sup>25</sup>

<sup>23</sup> [http://europa.eu/rapid/press-release\\_MEMO-16-2462\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm)

<sup>24</sup> [https://ec.europa.eu/info/law/law-topic/data-protection\\_de](https://ec.europa.eu/info/law/law-topic/data-protection_de)

<sup>25</sup> <https://haveibeenpwned.com/>

## **BSI-Sicherheitstest**

Bei einer Analyse von Botnetzen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) persönliche Daten von rund 18 Millionen Internet-Nutzern gefunden. Bei den Daten handelt es sich jeweils um Mail-Adressen und zugehörige Passwörter. Mit dem BSI-Sicherheitstest können Sie Ihren Mail-Zugang überprüfen, ob Sie Opfer von Cyberkriminellen sind.

[BSI-Sicherheitstest](#)<sup>26</sup>

## **HPI Identity Leak Checker**

Der „Identity Leak Checker“ des Hasso-Plattner-Instituts gleicht die angegebene E-Mail-Adresse mit einer Datenbank bekannt gewordener Leaks aus der Vergangenheit ab. Sollte sich Ihre Adresse zusammen mit anderen persönlichen Daten in einem der Datensätze finden, erhalten Sie diese Information umgehend per Mail.

[HPI Identity Leak Checker](#)<sup>27</sup>

## **Google Sicherheitscenter**

Einstellungen für Kontozugriff und Sicherheit bearbeiten. Jedes Google-Konto verfügt automatisch über die modernsten Sicherheitsfunktionen, so zitiert Google seine Sicherheitsgedanken.

[Sicher ins Web starten](#)<sup>28</sup>

## **Welche Prozesse und Dokumente muss ich in meinem Unternehmen überprüfen?**

Alle Punkte unterliegen einer erweiterten Rechenschaftspflicht: Die DSGVO rückt die Verantwortlichkeit von Unternehmen in den Vordergrund und führt erstmalig die Rechenschaftspflicht als zentralen Grundsatz der Datenverarbeitung auf. Sie sollten ein effektives Datenschutzmanagement-System mit den oben aufgeführten Prozessen in Ihrem Unternehmen integrieren und vor allem die einzelnen Schritte dokumentieren, sodass Sie – auch gegenüber einer Aufsichtsbehörde – nachweisen können, dass Sie geeignete Strategien und Maßnahmen ergriffen haben. Eine unzureichende Dokumentation der datenschutzrechtlichen Umsetzung der DSGVO kann sich maßgeblich auf die Höhe des Bußgeldtatbestands auswirken.

- Dokumentation der Datenverarbeitungsprozesse im Unternehmen (insbesondere Erweiterung der Dokumentationspflichten bei Auftragsverarbeitern, möglicherweise zusätzliche Dokumentationsanforderungen für Risk und Privacy Impact Assessment)
- Datenschutzerklärungen (Erweiterung der Informationspflichten)
- Einwilligungserklärungen (Verschärfung der formalen Vorgaben), Prozess für Widerruf der Einwilligung
- Anpassung der Betriebsvereinbarungen an DSGVO
- Prozesse zur Umsetzung von Widersprüchen
- Vereinbarungen zur Auftragsverarbeitung (Haftungsregelung, Dokumentation)
- Prozess bei Datenpannen entsprechend der neuen Vorgaben überarbeiten
- Verfahren, um Daten in gängigem elektronischen Format übertragen zu können

---

<sup>26</sup> <https://www.sicherheitstest.bsi.de/>

<sup>27</sup> <https://sec.hpi.uni-potsdam.de/leak-checker/search>

<sup>28</sup> <https://www.google.de/intl/de/safetycenter/everyone/start/>

- Durchführung von zielgruppengerechten Schulungen zu den Neuerungen der DSGVO und den eigenen Prozessen
- Einführung von Risk Assessment zur Festlegung geeigneter technisch-organisatorischer Maßnahmen
- Einführung von Privacy Impact Assessment
- Monitoring nationaler Gesetzgebung und Fortbildung

## Wie Sorge ich für Datensicherheit

Alle personenbezogenen Daten von Kunden und Mitarbeitern (auch Name oder E-Mail Adresse), egal ob auf Papier, PC oder Microfilm, müssen stärker als bisher, vor dem Zugriff Unbefugter geschützt werden.

Daten die nicht mehr benötigt werden, müssen vollständig gelöscht werden! Das gilt auch für Daten die mit einem Mindesthaltbarkeitsdatum (MHD) versehen und nach einer bestimmten Zeit gelöscht werden müssen. Papier Schreddern, auf elektronischen Datenträger, auch in Backups, unwiderruflich Löschen.

Alle Mitarbeiter des Unternehmens (Intern, Extern, Teilzeit), müssen über die Datenschutzverordnung in Kenntnis gesetzt und entsprechend geschult werden. Sie müssen eine entsprechende Erklärung unterschreiben, dass sie sich an die Datenschutz Vorschriften halten, und am besten auch bekanntgewordene Verstöße direkt an den DSB melden.

Ändern Sie regelmäßig Ihre Logins (Passworte), und nutzen Sie auf keinen Fall für alle Dienste das gleiche Passwort.

## Kette, Franchise, Kooperation

Sofern Sie kein [Einzelkämpfer](#)<sup>29</sup> sind, werden Sie bestimmt von Ihrer Organisation nicht alleine gelassen. In den kommenden Wochen und Monaten werden bestimmt einige Seminare, Online-Schulungen und Merkblätter zum Thema angeboten. Diese sollten unbedingt wahrgenommen werden, der 25. Mai 2018 kommt schneller als man denkt.

**Hinweis:** Bei Verstößen, auch bei Mitgliedern einer Kette, Franchise oder Kooperation, haftet jeder Unternehmer, für sich selbst!

## Praxisbeispiel

Sie versenden gerne **Weihnachtskarte oder Geburtstagsglückwünsche**, man freut sich ja über jede nett gemeinte Geste, so auch Frau Mustermann?

Frau Mustermann freut sich jedoch gar nicht über die lieb gemeinte Post, und hat auch nie zugestimmt. Sie hat das Recht Widerspruch beim Unternehmer einzulegen, oder was schlimmer wäre, diesen gleich bei der Datenschutzbehörde!

Der Betroffene kann insbesondere Datenverarbeitungen zu Zwecken des Direktmarketings, einschließlich der Profilbildung für diese Zwecke, widersprechen.

## ePrivacy Verordnung (ePV)

Die ePrivacy Verordnung (ePV) baut auf der EU-DSGVO auf und soll deren Regelungsbereich

---

<sup>29</sup> <https://business-view.photo/jobs/>



spezifisch ergänzen. Sie soll die Vertraulichkeit in der elektronischen Kommunikation sicherstellen und den Umgang mit personengezogenen Daten im Online-Bereich regeln.

Nach aktuellem Stand tritt die ePV voraussichtlich zusammen mit der EU-DSGVO am 25. Mai 2018 in Kraft und erweitert deren Regelungswerk. Jeder datenbasierte Informationsaustausch ist betroffen, auch von Rechner zu Rechner.

Kontrolle über die Daten: Der Nutzer muss der Verwendung seiner Daten ausdrücklich zustimmen (Opt-in), nur dann dürfen Cookies oder andere Identifier eingesetzt werden.

Privacy Einstellung im Browser: Es ist zu erwarten, dass die Browserhersteller Lösungen für die ePV in ihren Browsern bereitstellen werden. Die wird aber nur Funktionieren, wenn der [Browser up-to-date](#)<sup>30</sup> ist!

## Cloud / Webspace

Quelle: [DEin halbfertiges Fotobuch](#)<sup>31</sup> - ISBN 9783737523387

Unter Cloud Computing (deutsch etwa: Rechnen in der Wolke) versteht man das Speichern von Daten in einem entfernten Rechenzentrum beziehungsweise Festplatte (umgangssprachlich: „Ich lade das Bild mal in die Cloud hoch.“), aber auch die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind, sondern eben in der (metaphorischen) Wolke (englisch cloud).



Der Zugriff auf die entfernten Systeme erfolgt über ein Netzwerk, beispielsweise das des Internet. Es gibt aber im Kontext von Firmen auch sogenannte „Private Clouds“, bei denen die Bereitstellung über ein firmeninternes Intranet erfolgt.

**Daten fallen nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG), falls sie keinen Personenbezug aufweisen.** Dies gilt etwa für statistische Auswertungen, technische Zeichnungen oder Warenverzeichnisse. Derartige Informationen können ohne datenschutzrechtliche Probleme auf jedem System verarbeitet und gespeichert werden, also auch in der Cloud.

Wenn personenbezogene Daten Dritter in die Cloud gegeben werden, müssen sich beispielsweise deutsche Auftraggeber vorab und anschließend regelmäßig nachvollziehbar vor Ort in der Cloud davon überzeugen, dass die Vorgaben des Bundesdatenschutzgesetzes eingehalten werden. Weil namhafte Cloud-Anbieter Datenbestände ihrer Kunden weitergeben, drohen den Kunden Bußgelder. Cloud-Betreiber mit Sitz in den USA unterliegen dem US-Recht und demnach dem Patriot Act. Unternehmen mit Sitz in den USA sind deshalb gezwungen, auch Daten an amerikanische Behörden auszuliefern, die sich auf Servern in fremdem Hoheitsbereich befinden. Dies ist beispielsweise von **Amazon, Microsoft und Google** bestätigt worden.

Aber meistens fängt es ja gerade mit dem gemeinsamen Kalender und Adressbuch an. Grundsätzlich gilt, dass das BDSG greift, sobald es sich bei den genutzten Inhalten um personenbezogene Daten handelt, also "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person". Ein Verstoß liegt folglich bereits vor, wenn die Sekretärin eines Fotografen ihrem Chef Termine mit Adressen und Telefonnummern der Kunden in den Google-Kalender einträgt oder ihm die Daten per Mail an seinen Google-Mail-Account schickt.

Lässt man fremde Daten von externen Anbietern verarbeiten, handelt es sich dabei üblicherweise um eine sogenannte Auftragsdatenverarbeitung. §11 BDSG.

<sup>30</sup> <https://business-view.photo/wuerden-sie-ohne-schutz-durch-ein-minenfeld-laufen/>

<sup>31</sup> <https://business-view.photo/?p=10108>

## BDSG §9 (Technische und organisatorische Maßnahmen)

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

[http://www.gesetze-im-internet.de/bdsg\\_1990/\\_9.html](http://www.gesetze-im-internet.de/bdsg_1990/_9.html)

Weitere Informationen: [www.spiegel.de/netzwelt/web/cloud-dienste-datenschutz-in-der-wolke-a-783446.html](http://www.spiegel.de/netzwelt/web/cloud-dienste-datenschutz-in-der-wolke-a-783446.html)

Service	Beschreibung / Link	Onlinespeicher / Preise		Bemerkungen
flickr	<a href="http://www.flickr.com/">www.flickr.com/</a>	1 TB	./.	Nur für Fotos
Dropbox	Pro erworbenen Freund, gibt es 50MB Onlinespeicher Gratis dazu <sup>32</sup> <a href="https://business-view.photo/go/dropbox/">https://business-view.photo/go/dropbox/</a>	2 GB		Durch persönliche Links können Dateien und Order freigegeben werden.
		1 TB	9,99 EUR/mtl	
Google Drive	<a href="http://drive.google.com/">http://drive.google.com/</a>	15 GB	./.	Google Drive unterstützt über 30 verschiedene Dateiformate, die direkt im Browser geöffnet werden können. Dazu zählen neben den Google-eigenen Dateitypen etwa auch Photoshops .PSD, PDF oder Video
		100 GB	1,99 \$/Monat	
		1 TB	9,99 \$/Monat	
		10 TB	99,99 \$/Monat	
		20 TB	199,99 \$/Monat	
		30 TB	299,99 \$/Monat	
Wuala	<a href="http://www.wuala.com">www.wuala.com</a>	5 GB	./.	Daten werden vor Upload ins Internet verschlüsselt <sup>33</sup>
SkyDrive	<a href="https://onedrive.live.com/">https://onedrive.live.com/</a>	7 GB	./.	Cloud-Speicher von Microsoft <sup>34</sup>
iCloud		5 GB	./.	
		20 GB	1 EUR/mtl.	
		200 GB	4 EUR/mtl.	
<b>↓ Europäische / Deutsche Services ↓</b>				
α-drive	<a href="https://business-view.photo/go/cloud/">https://business-view.photo/go/cloud/</a>	max 100 GB	0,00 <sup>35</sup>	Gratis zu Webhosting, bis zu 100 GB Speicherplatz inklusive
Telekom Cloud	<a href="http://www.telekom.de/telekomcloud">www.telekom.de/telekomcloud</a>	25 GB	./.	Zur Nutzung ist es nicht nötig Kunde der Telekom sind
HiDrive	<a href="https://business-view.photo/go/onlinespeicher/">https://business-view.photo/go/onlinespeicher/</a>	500 GB	14,90 EUR/mtl.	30 Tage kostenlos testen

32 Bieten Sie Ihren Kunden, doch den Express Service, keine Versandzeit an. Senden Sie dem Kunden Ihren Werbelink zu Dropbox, dieser Meldet sich an, und erstellt ein Verzeichnis (Firmenname / Kd.-Nr. / Re.-Nr.) und gibt Ihnen dieses Frei. So können Sie die bearbeiteten Daten bequem Übertragen und haben 50MB mehr Onlinespeicher.

33 Bei Dropbox & Co. benötigen Sie Zusatz-Software wie BoxCryptor, um Ihre Daten zu verschlüsseln. ([www.boxcryptor.com](http://www.boxcryptor.com))

34 Microsoft arbeitet in Deutschland, seit 2015, mit der Telekom zusammen, und will so eine „deutsche“ Lösung anbieten

35 Je nach Webhosting Paket, welche nicht kostenlos sind.

ownCloud	<a href="http://www.owncloud.org">www.owncloud.org</a>	./.	./.	Hier betreiben Sie Ihre eigene Cloud-Festplatte. Sie benötigen nur Internet-Speicherplatz, sogenannten Webspace.
SWINDI	<a href="http://www.swindi.de">www.swindi.de</a>			Fotograf erstellt ein Album, mit Login, Bearbeiter brauchen nur einen Link um zusätzliche Fotos hochzuladen. Fotograf muss die Fotos freigeben
Fotoalbum	<a href="http://www.business-view.photo/?p=12462">www.business-view.photo/?p=12462</a>	./.	./.	Für den/die Private eigene Webseite

Tabelle 1: Cloud / Webspeicher (Stand Okt. 2017)

## Zusätzliche Informationen & Quellen

- Bitkom Auftragsdatenverarbeitung: [Mustervertragsanlage zur Auftragsdatenverarbeitung](#)<sup>36</sup>.
- Bitkom Dokumentationspflichten: Leitfaden: Das [Verfahrensverzeichnis BDSG](#)<sup>37</sup> – Ein Praxisleitfaden (Version 3.0).
- Bitkom [Leitfaden Übermittlung personenbezogener Daten](#)<sup>38</sup> – Inland, EU-Länder, Drittländer
- [Safe-Harbor-Urteil](#)<sup>39</sup> des EuGH und die Folgen. Fragen und Antworten.
- Übersicht [DSGVO](#)<sup>40</sup> mit Erwägungsgründen
- BvD: [Datenschutz-Grundverordnung](#)<sup>41</sup> (DSGVO) als Website übersichtlich dargestellt
- Oppenhoff & Partner: [Synopsis Übersicht BDSG](#)<sup>42</sup> / DSGVO
- Wybitul/Böhm: [Das neue Datenschutzrecht](#)<sup>43</sup> (Juli 2016) – Folgen für Compliance und interne Ermittlungen

# Formulare – Ausfüllhinweise und Anwendung

Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)  
Verantwortlicher

**Verarbeitungstätigkeit - Formblatt (PDF Ausfüllbar)**  
<https://business-view.photo/formblatt-verarbeitungstaetigkeit/>

36 <https://www.bitkom.org/Bitkom/Publikationen/Aktualisierte-Mustervertragsanlage-zur-Auftragsdatenverarbeitung.html>

37 <https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Das-Verfahrensverzeichnis.html>

38 <https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender.html>

39 <https://www.bitkom.org/Bitkom/Publikationen/Safe-Harbor-Entscheidung-des-EuGH.html>

40 <http://www.privacy-regulation.eu/de/index.htm>

41 <https://dsgvo-gesetz.de/>

42 [http://www.oppenhoff.eu/files/oppenhoff/downloads/dokumente/Synopse%20BDSG%20zu%20EU-DSGVO\\_Oppenhoff\\_Partner\\_Mai\\_2016.pdf](http://www.oppenhoff.eu/files/oppenhoff/downloads/dokumente/Synopse%20BDSG%20zu%20EU-DSGVO_Oppenhoff_Partner_Mai_2016.pdf)

43 <http://hoganlovells-blog.de/2016/07/06/das-neue-eu-datenschutzrecht-folgen-fuer-compliance-und-interne-ermittlungen/>

Es wird darauf hingewiesen, dass es sich hier um ein fiktives Beispiel handelt. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen.

## **Inhaltsverzeichnis Formulare**

- A) Stammdatenblatt
- B) Datenverarbeitungen/Datenverarbeitungszwecke
- C) Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung
- D) Detailangaben zu (2) Personalverwaltung
- E) Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

### **A. Stammdatenblatt**

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

- (a) Name(n) und Anschrift(en):

*Max Mustermann GmbH  
Neuer Weg 1  
DE-XXXXX Musterdorf*

- (b) E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.):

*max@example.com*

- (c) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Datenschutzbeauftragten<sup>44</sup>:

*Franz Fachmann RA  
Datenstraße 5  
AT-YYYYY Datenstadt*

- (d) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Vertreters des (der) Verantwortlichen:<sup>45</sup>

*KEINER*

---

<sup>44</sup> Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. HINWEIS: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „Datenschutzbeauftragter“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (z.B. „Datenschutzkoordinator“). Dieser kann, muss aber nicht ins Verfahrensverzeichnis aufgenommen werden. Siehe dazu das zur Auslegung der Bestimmungen zum Datenschutzbeauftragten in der DSGVO sowie zu dessen Aufgaben können die Guidelines der Art 29-Gruppe zum Datenschutzbeauftragten herangezogen werden, die auf der Website der EU-Kommission abrufbar sind. [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

<sup>45</sup> Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

## B. Datenverarbeitungen/Datenverarbeitungszwecke

- (a) Zwecke und Beschreibung der Datenverarbeitung<sup>46</sup>:
1. Rechnungswesen und Geschäftsabwicklung: Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenzen oder Verträge) in diesen Angelegenheiten
  2. Personalverwaltung: .....
  3. Marketing: .....
  4. Geschäftspartnerdatenbank: .....
  5. usw.

- (b) Wurde eine Datenschutz-Folgenabschätzung durchgeführt?<sup>47</sup>

Ja  Nein

Wenn Ja, wann?

*zuletzt vor 6 Monaten*

Wenn Nein, aus welchem Grund nicht?<sup>48</sup>

---

46 Zum Begriff „Verarbeitung“; sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.

47 Zur Datenschutz-Folgenabschätzung im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen.

48 Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch „Risiko-Folgenabschätzung“. Download 20 Seiten PDF – Was muss getan werden? <https://business-view.photo/?p=14293>

## C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung

### (a) Kategorien der betroffenen Personen

Lfd.Nr. Beschreibung der Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Lieferanten usw.)

1. Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
2. Sachbearbeiter beim Verantwortlichen
3. An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten

### (b) Rechtsgrundlagen<sup>49</sup>

#### 1. Art 6 Abs 1 lit

a Einwilligung der Betroffenen (Freiwillig, ohne Vorauswahl)

b zur Vertragserfüllung erforderlich

c gesetzliche Verpflichtungen nach Handels- und Steuerrecht

f berechnigte Interessen des Verantwortlichen

DSGVO

- AT<sup>50</sup> → § 132 BAO, §§ 190, 212 UGB
- DE<sup>51</sup> → § 147 Abs. 2 i. V. m. Abs. 1 Nr.1, 4 und 4a AO, § 14b Abs. 1 UStG

### (c) Verträge , Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten<sup>52</sup>) sind abgelegt:<sup>53</sup> (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen in der Verkaufsabteilung, Rechnungen (auch) in der Finanzabteilung, erledigte Geschäftsfälle im Archiv. Verträge mit Auftragsverarbeitern sind, je nach Thematik, in der Rechtsabteilung, Finanzabteilung, Vertriebsabteilung oder IT-Abteilung abgelegt.

### (d) Kategorien der verarbeiteten Daten und Lösungs- bzw. Aufbewahrungsfristen<sup>54</sup>

1. Kategorien der verarbeiteten Daten und Ankreuzen, ob sie an Empfänger übermittelt werden

---

49 Die Rechtsgrundlagen (z.B. rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verfahrensverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung“.

50 Österreich → <https://www.jusline.at/bundesgesetze>

51 Deutschland → <https://www.gesetze-im-internet.de/>

52 Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

53 Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung).

54 Nach der DSGVO sind die Lösungsfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verfahrensverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Lösungsfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (z.B. „nach Ablauf des Vertrages“).



Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien <sup>55</sup>  iSd Art 9 DSGVO <sup>56</sup>  strafrechtlich relevant iSd Art 10 DSGVO <sup>57</sup>	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (z.B. Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
a	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x	x
	2	Anschrift	Nein	x	x	x	x	x	x	x	x	x	x
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	x	x	x	x	x	x	x	x	x	x
	4	Firmenbuchdaten	Nein	x	x	x	x	x	x	x	x	x	x
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		x		x						
	6	Bankverbindungen	Nein	x	x	x	x	x	x	x	x	x	
	7	Kreditkartennummern und -unternehmen	Nein	x	x	x	x						
	8	UID/TAX/VAT Nr.	Nein	x	x	x	x	x	x	x	x	x	
	9	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	x	x
	10	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift oä.)	Nein	x	x	x	x	x	x	x	x	x	x
	11	Vertragstexte und Geschäftskorrespondenzen	Nein	x	x	x	x	x	x	x		x	
b	12	Name	Nein	x	x	x	x	x	x	x	x	x	x
	13	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	Nein	x	x	x	x	x	x	x	x	x	x
	14	Vom betroffenen Sachbearbeiter bearbeitete Fälle	Nein	x	x	x	x	x	x	x	x	x	x
	15	Umfang der Vertretungsbefugnis	Nein	x	x	x	x	x	x	x	x	x	x
c	16	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x	x
	17	Anschrift	Nein	x	x	x	x	x	x	x	x	x	x
	18	Kontaktdaten (Tel., Mail, Fax)	Nein	x	x	x	x	x	x	x	x	x	x
	19	Firmenbuchdaten	Nein	x	x	x	x	x	x	x	x	x	x

55 Verarbeitung von „sensiblen Daten“ ist untersagt und nur in Ausnahmefällen möglich. DSGVO: Art 4, Art 8, Art 9, Art. 10

56 Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten“): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

57 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen unter behördlicher Aufsicht.

20	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	x	x	x
21	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift oä.)	Nein	x	x	x	x	x	x	x	x	x	x	x
22	UID/TAX/VAT Nr.	Nein	x	x	x	x	x	x	x	x	x	x	x
23	Bankverbindungen	Nein	x	x	x	x	x	x	x	x	x		
24	Kreditkartennummern und -unternehmen	Nein	x	x	x	x							
25	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		x	x	x							

1. Lösungs- und Aufbewahrungsfristen (wenn möglich)

Zu Beachten ist hier auch, das die Daten in einem evtl. IT-Backup unwiederbringlich gelöscht werden!

Daten aus (d)1 (Lfd. Nr.)	Angabe bzw. Beschreibung der Lösungs- bzw. Aufbewahrungsfristen
1-4; 6-24; 26;	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 10 Jahre <sup>58</sup> ; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
5; 25;	Bis zur Beendigung der Geschäftsbeziehungen

(c) Kategorien von Empfängern<sup>59</sup>, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern<sup>14</sup>

1. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie z.B. UNO, OSZE)

Empfängerkategorien aus (d)1	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsvertreter im Geschäftsfall		
Wirtschaftstreuhänder		
Gerichte		
Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer (z.B. Leasing)		
mitwirkende Vertrags- und Geschäftspartner		
Versicherungen um Anlassfall		
Provider (IT-Dienstleister)		

<sup>58</sup> Je EU-Land unterschiedlich, in „Verarbeitungstätigkeit“ ist ein Entsprechender Hinweis DE, AT... auswählbar

<sup>59</sup> Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

2. Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):<sup>60</sup>

(d) Angemessenheitsbeschluss der Europäischen Kommission<sup>61</sup>, gibt es für folgende Länder:

Kanada

## C. Detailangaben zu (2) Personalverwaltung

...

## D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

HINWEIS: die hier angeführten Maßnahmen verstehen sich als beispielhafte Auflistung; es ist je nach Einzelfall und Risikobehaftung der Datenverarbeitung zu entscheiden, welche konkreten Maßnahmen zu treffen sind und welche im Einzelfall auch zumutbar sind!

- (a) Vertraulichkeit:
  1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
  2. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
  3. iZugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Protokollierung von Zugriffen; oder: Zugriff nur für Unternehmensinhaber, Mitarbeiter der Abteilung Rechnungswesen und Mitarbeiter, die

---

<sup>60</sup> Während der Datenverkehr innerhalb der EU aufgrund des durch die DSGVO gewährleisteten gleichen Datenschutzniveaus keinen Beschränkungen unterliegt, ist der Datenverkehr mit Drittländern (oder internationalen Organisationen) nur unter folgenden Voraussetzungen zulässig: Zunächst muss die Datenverarbeitung im Inland (innerhalb der EU) den Vorgaben der DSGVO entsprechen. Dieses unionsweit gewährleistete Schutzniveau für natürliche Personen darf bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden. Dasselbe gilt auch dann, wenn aus einem Drittland (oder von einer internationalen Organisation) personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland (bzw internationale Organisation) weiterübermittelt werden. Die DSGVO nennt folgende Fälle einer zulässigen Datenübermittlung an ein Drittland bzw eine internationale Organisation: DSGVO: Art 44-49 Relevante Erwägungsgründe: 101-115

<sup>61</sup> FAQ EU: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu\\_de](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_de)

an der Geschäftsabwicklung beteiligt sind

(b) Integrität:

1. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
2. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

(c) Verfügbarkeit und Belastbarkeit:

1. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie, Virenschutz, Firewall;

(d) Pseudonymisierung und Verschlüsselung:

1. Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
2. Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt: ....

(e) Evaluierungsmaßnahmen:

1. Datenschutz-Management (z.B. Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;

<b>DSGVO</b> Datenschutz-Grundverordnung <b>GDPR</b> General Data Protection Regulation	<b>Verarbeitungstätigkeit:</b>  <b>Benennung:</b> _____		Lfd. Nr.:
Datum der Einführung:		Datum der letzten Änderung:	
Verantwortliche Fachabteilung (Art. 30 Abs. 1 S. 2 lit a) <i>Ansprechpartner</i> <i>Adresse</i> <i>Telefon</i> <i>E-Mail-Adresse</i>			
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)			
Optional: Name des eingesetzten Verfahrens			
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input type="checkbox"/> Kunden <input type="checkbox"/> Dienstleister <input type="checkbox"/> Patienten		

<p>Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)</p>	<p><input type="checkbox"/> Firma / Gesellschaftsform  <input type="checkbox"/> Adresse  <input type="checkbox"/> Name  <input type="checkbox"/> GF/Inhaber    <input type="checkbox"/> AP/MA    <input type="checkbox"/> .....    <input type="checkbox"/> .....</p> <p><input type="checkbox"/> Kontaktangaben  <input type="checkbox"/> Allg. Telefon    <input type="checkbox"/> Durchwahl    <input type="checkbox"/> Telefax    <input type="checkbox"/> Mobil  <input type="checkbox"/> E-Mail GF    <input type="checkbox"/> E-Mail AP    <input type="checkbox"/> E-Mail (Allg.)    <input type="checkbox"/> .....</p> <p><input type="checkbox"/> Geburtsdatum  <input type="checkbox"/> Bank  <input type="checkbox"/> Branche</p> <p>Besondere Kategorien personenbezogener Daten (Art. 9/10) „sensible Daten“:  <input type="checkbox"/>  <input type="checkbox"/></p>
<p>Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)</p>	<p><input type="checkbox"/> intern (Zugriffsberechtigte) Abteilung/ Funktion</p> <hr/> <p><input type="checkbox"/> extern Empfängerkategorie</p> <hr/> <p><input type="checkbox"/> Drittland oder internationale Organisation (Kategorie)</p> <hr/> <p><input type="checkbox"/> Behörde National (Finanzamt / Gericht / Behörde / Inkassounternehmen)</p>
<p>ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)</p> <p>Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt.</p>	<p><input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant  <input type="checkbox"/> Datenübermittlung findet wie folgt statt:</p> <hr/> <p><input type="checkbox"/> Drittland oder internationale Organisation (Name)</p> <hr/> <p><input type="checkbox"/> Angemessenheitsbeschluss der Europäischen Kommission</p> <hr/> <p><input type="checkbox"/> Dokumentation geeigneter Garantien</p>
<p>Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)</p>	<p><input type="checkbox"/> 10+1 Jahre, Rechnung / Mahnung;  darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen (§ 147 Abs. 2 i. V. m. Abs. 1 Nr.1, 4 und 4a AO, § 14b Abs. 1 UStG)</p> <p><input type="checkbox"/> 6+1 Jahre, Handels- oder Geschäftsbriefe  <input type="checkbox"/> Unbestimmt, da erst nach dem Ende der Vertragsdauer / Lebensende beginnt  <input type="checkbox"/> 30+1 Jahre  <input type="checkbox"/> Bis zur Beendigung der Geschäftsbeziehungen  <input type="checkbox"/> .....</p>
<p>Rechtsgrundlage für Datenerhebung (Art 6 Abs 1 lit)</p>	<p><input type="checkbox"/> Einwilligung der Betroffenen  <input type="checkbox"/> zur Vertragserfüllung erforderlich  <input type="checkbox"/> gesetzliche Verpflichtungen nach der BAO und dem UGB  <input type="checkbox"/> berechnete Interessen des Verantwortlichen DSGVO § 132 BAO, §§ 190, 212 UGB</p>

<p>Verträge , Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten) sind abgelegt:</p>	<p>Unterlagen zu aufrechten Geschäftsabwicklungen, sind abgelegt</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Verkaufsabteilung</li> <li><input type="checkbox"/> Rechnungen (auch) in der Finanzabteilung</li> <li><input type="checkbox"/> erledigte Geschäftsfälle .....</li> </ul> <p>Verträge mit Auftragsverarbeitern sind abgelegt</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Rechtsabteilung</li> <li><input type="checkbox"/> Finanzabteilung</li> <li><input type="checkbox"/> Vertriebsabteilung</li> <li><input type="checkbox"/> IT-Abteilung</li> <li><input type="checkbox"/> Öffentlich</li> </ul>	
<p>Ablaufbeschreibung Datennutzung</p>		
<p>Hinweise / Bemerkungen / Datenschutzerklärung / Vertragstext</p>		
<p>Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8</p>		
<p>..... Verantwortlicher</p>	<p>..... Datum</p>	<p>..... Unterschrift</p>



# Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO<sup>62</sup>,

Hinweis: Diese Formulierungshilfe ist nicht abschließend und bezieht sich in erster Linie auf die Fallgestaltung einer Auslagerung von klassischen IT-Dienstleistungen z. B. für die Lohnabrechnung oder Finanzbuchhaltung. Je nach konkretem Anwendungsfall müssen gegebenenfalls weitere Inhalte hinzukommen, können solche weggelassen oder müssen modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden (z. B. bei Berufsgeheimnisträgern, bei Dienstleistungen zur Wartung, Datenlöschung oder -konvertierung, bei der externen Datenarchivierung)

Verantwortlicher (Auftraggeber):

.....  
Auftragsverarbeiter (Auftragnehmer):

.....

## 1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

.....

.....  
*(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen)*

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Der Vertrag beginnt am ..... und endet am .....

---

<sup>62</sup> Die konkrete Ausgestaltung ist an den jeweiligen Sachverhalt anzupassen. Diese Formulierungshilfe stellt keine Standardvertragsklauseln im Sinne von Art. 28 Abs. 8 DSGVO dar.

oder

wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist .....

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

.....  
(nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.)

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

.....  
Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

.....  
Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

3. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Verantwortliche ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregel-

mäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

#### 4. Weisungsberechtigte des Verantwortlichen, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Personen des Verantwortlichen sind:

.....  
(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragsverarbeiter sind:

.....  
(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

.....  
(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

#### 5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.

Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Verantwortlichen verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Verantwortli-

chen insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Das Ergebnis der Kontrollen ist zu dokumentieren.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben dem Verantwortlichen unverzüglich an folgende Stelle weiterzuleiten:

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen nach Überprüfung bestätigt oder geändert wird.

Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Unabhängig davon hat der Auftragsverarbeiter personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DSGVO zugrunde liegt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Verantwortlichen beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

Der Verantwortliche kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DSGVO durch den Auftragsverarbeiter als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen. Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Verantwortlichen gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für

die-sen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Verantwortlichen obliegen:

.....  
(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, etc.)

Berufsgeheimnisträger haben den Auftragsverarbeiter zusätzlich zu diesem Vertrag zur Verschwiegenheit nach § 203 Abs. 4 StGB zu verpflichten.

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz Herr/Frau

.....  
(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

Oder

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

Sofern einschlägig:

Der Auftragsverarbeiter verpflichtet sich den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

#### 6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

## 7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Hinweis: Hier sind verschiedene Regelungsalternativen möglich. Die Parteien können ein absolutes Unterauftragsverbot vereinbaren, es kann aber auch ein Verbot mit Genehmigungsvorbehalt im Einzelfall geregelt werden. Auf letztere Möglichkeit bezieht sich der unten stehende Formulierungsvorschlag.

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Verantwortlichen ist dem Auftragsverarbeiter nur mit Genehmigung des Verantwortlichen gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter dem Verantwortlichen Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragsverarbeiter dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Verantwortlichem und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat. Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragsverarbeiter die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der

Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

Hier haben die Vertragsparteien einen Gestaltungsspielraum: Entweder werden dem Auftragsverarbeiter allgemein Befugnisse eingeräumt, Subunternehmer zu beauftragen oder dies wird von einer Einzelgenehmigung abhängig gemacht. Einigt man sich auf eine allgemeine Befugnis des Auftragsverarbeiters zur Beauftragung von Subunternehmern, ist jede Subbeauftragung vorher durch den Auftragsverarbeiter dem Verantwortlichen anzuzeigen. Der Verantwortliche hat dann von Gesetzes wegen ein Recht auf Einspruch gegen diese Änderung (Art. 28 Abs. 2). Das Recht des Verantwortlichen zum Einspruch ist im Vertrag ausdrücklich zu erwähnen. Da das Gesetz die Folgen dieses Einspruchs nicht regelt, wird empfohlen, hierzu vertragliche Regelungen zu finden. Wird keine Regelung getroffen, ist die Bestellung des Unter-Auftragsverarbeiters, gegen den Einspruch erhoben wurde, nicht möglich.

## 8. Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung gewährleistet. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DSGVO wie Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (Art. 28 Abs. 3 lit. c). Die Formulierung in Art. 32 Abs. 1 DSGVO „diese Maßnahmen schließen unter anderem Folgendes ein“ verdeutlicht andererseits, dass die dort vorgenommene Aufzählung nicht abschließend ist. Für die Auftragsverarbeitung sind auch technische und organisatorische Maßnahmen umzusetzen, die in Kapitel III der DSGVO genannten Rechte der betroffenen Personen wahren (Art. 28 Abs. 3 lit. e). Diese Maßnahmen sollen u. a. sicherstellen, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (Transparenz) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

Beispiele für typische, bewährte technische und organisatorische Maßnahmen in den einzelnen Bereichen können den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO“ (Abschnitte 6.7 bis 6.9) entnommen werden. Die Auflistung dort ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein.

### 8.3 Methodik der Risikobewertung

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobeurteilung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

.....



.....  
Das im Anhang ..... beschriebene Datenschutz- und Datensicherheitskonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum Datensicherheitsrisiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Zweckbindung, Transparenz und Intervenierbarkeit detailliert und unter besondere Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar.

Das im Anhang ..... beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird als verbindlich festgelegt.  
Folgende Möglichkeit für den Nachweis durch Zertifizierung bestehen:  
Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Datensicherheitsmaßnahmen des Auftragsverarbeiters wurden am ..... durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Zertifizierungen nach Art. 42 :

.....  
.....  
Diese vollständigen Prüfunterlagen und Auditberichte können vom Verantwortlichen jederzeit eingesehen werden.

Oder:

Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (siehe Abschnitt 8) und das Ergebnis samt vollständigem Auditbericht dem Verantwortlichen mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich.

Die Datensicherheitsmaßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Sicherheitsstandards nicht unterschreiten.

Wesentliche Änderungen sind vom Auftragsverarbeiter mit dem Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

#### 9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz so-wie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen.

Oder

wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

.....

Die Löschung bzw. Vernichtung ist dem Verantwortlichen mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

#### 10. Vergütung

.....

.....

#### 11. Haftung

.....

.....

Auf Art. 82 DSGVO wird verwiesen.

Im Übrigen wird folgendes vereinbart:

.....

.....

.....

#### 12. Vertragsstrafe

Bei Verstoß des Auftragsverarbeiters gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro vereinbart.

#### 13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Weitere Beispiele für mögliche Regelungen:

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.



# Wichtige Hinweise

Ich/Wir übernehmen keine Gewähr für die Aktualität, Vollständigkeit und Richtigkeit der bereitgestellten Informationen. Dies bezieht sich auf eventuelle Schäden materieller oder ideeller Art Dritter, die durch die Nutzung dieses Dokumentes, oder der beschriebenen Techniken verursacht wurden.

Über eine Rückmeldung würden wir uns freuen. Wünsche, Anregungen, Erfahrungen bei der Arbeit mit den Unterlagen werden gerne entgegengenommen. Bitte auch nicht mit Kritik sparen.

<https://business-view.photo/?p=1682> #dsvgo #handbuch

Gerichtsurteile und rechtliches dienen nur Informationszwecken und erheben keinen Anspruch auf Vollständigkeit. Die Artikel / Links zu Recht und verwandten Themen dienen der allgemeinen Bildung und Weiterbildung und nicht der Beratung im Falle eines individuellen rechtlichen Anliegens. Wie alle Projektbereiche sind sie ständigen Veränderungen unterworfen. Diese Artikel / Links entstehen offen und ohne redaktionelle Begleitung und Kontrolle. Es ist möglich, dass Sie hier auf unrichtige, unvollständige, veraltete, widersprüchliche, in falschem Zusammenhang stehende oder verkürzte Angaben treffen. Das gilt auch für Texte auf Diskussions-, Hilfe- und sonstigen Internet Seiten, zu dieser Publikation.

## Internet Verweise / Links

Bei "Links" handelt es sich stets um "lebende" (dynamische) Verweisungen. Der/die Autor(en) hat bei der erstmaligen Verknüpfung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Er überprüft aber die Inhalte, auf die er in seinem Angebot verweist, nicht ständig auf Veränderungen, die eine Verantwortlichkeit neu begründen könnten. Wenn festgestellt wird oder von anderen darauf hingewiesen wird, dass ein konkretes Angebot, zu dem er einen Link bereitgestellt hat, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst, wird der Verweis auf dieses Angebot aufgehoben, und in den Social Media Kanälen des Autors bekannt gegeben.

# Inhaltsverzeichnis

DATENSCHUTZ-GRUNDVERORDNUNG DSGVO.....	1
Immer auf der sicheren Seite.....	2
Was Unternehmen und Admins jetzt tun müssen.....	2
Für mein Business, Geschäft, Praxis, Gaststätte?.....	2
Was auf Geschäftsführung und Admins zukommt. ....	3
Was sind personenbezogene Daten?.....	3
Keine Datenverarbeitung ohne Rechtsgrundlage.....	4
Komplizierte Einwilligung.....	4
Informiert und freiwillig zustimmen.....	5
Dokumentations-, Nachweis- und Rechenschaftspflichten.....	5
Weitergabe personenbezogener Daten und Outsourcing der Verarbeitung an Dritte.....	6
Permanente Auskunftspflicht.....	7
Datenschutz "by Design" und "by Default".....	7
take it or leave it.....	8
Neue Datenschutzerklärung.....	8
Fazit.....	8
Was ist zu tun? - Die Bürokratie des Grauens!.....	9
Was ist neu? Was muss beachtet werden?.....	9
Datenschutzbeauftragte (DSB).....	12
Datenpanne? Was nun?.....	12
Wurde ich gehackt? Jetzt den Selbst-Check machen!.....	12
Welche Prozesse und Dokumente muss ich in meinem Unternehmen überprüfen?.....	13
Wie Sorge ich für Datensicherheit.....	14
Kette, Franchise, Kooperation.....	14
Praxisbeispiel.....	14
ePrivacy Verordnung (ePV).....	14
Cloud / Webspace.....	15
BDSG §9 (Technische und organisatorische Maßnahmen).....	16
Zusätzliche Informationen & Quellen.....	17
Formulare – Ausfüllhinweise und Anwendung .....	17
Inhaltsverzeichnis Formulare.....	18
A. Stammdatenblatt.....	18
B. Datenverarbeitungen/Datenverarbeitungszwecke.....	19
C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung.....	20
C. Detailangaben zu (2) Personalverwaltung.....	23
D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen.....	23
Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO,.....	27
Wichtige Hinweise.....	37
Notizen.....	39



# CATEGORIES OF PERSONAL INFORMATION

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.



Provided by [www.enterprivacy.com](http://www.enterprivacy.com)