Datenschutz-Grundverordnung

# DSGVO: Darauf sollten Sie achten

❶ Im Fokus der DSGVO steht der Schutz persönlicher digitaler und analoger Daten.

Bild: Deutsche Messe AG / CeBIT

## KOMPAKT INFORMIEREN

**Die in allen EU-Mitgliedstaaten verbindlich geltende Datenschutz-Grundverordnung (DSGVO) legt fest, wie private Unternehmen und öffentliche Stellen personenbezogene Daten sammeln, speichern und nutzen dürfen.**

**Darüber hinaus regelt sie Auskunfts-, Dokumentations-, Anzeige- und andere Pflichten gegenüber Betroffenen und Behörden.**

**Ergänzt wird die DSGVO durch das neu gefasste Bundesdatenschutzgesetz (BDSG-neu), das die DSGVO an das deutsche Datenschutzrecht anpasst. Die DSGVO ersetzt die seit 1995 geltende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.**

### Wichtiger Hinweis

**Dieser Artikel gibt den Recherchestand des Autors zur aktuellen Rechtslage wieder. Für eventuell enthaltene Fehler wird keine rechtliche Verantwortung übernommen. Da spezielle Umstände oder individuelle Fallkonstellationen ebenso wenig berücksichtigt werden können, wie die künftige rechtliche Auslegung und praktische Anwendung der teilweise allgemein formulierten DSGVO-Bestimmungen, wird die Beratung durch einen externen Datenschutzexperten empfohlen.**

Seit dem 25. Mai 2018 gilt die neue Datenschutz-Grundverordnung (DSGVO). Sie ist für alle Unternehmen verbindlich und betrifft damit auch TGA-Planungsbüros, Gebäude-Energieberater und Handwerksbetriebe. Was die DSGVO vorgibt und worauf man achten sollte, beschreiben die folgenden Absätze.

Nach einer zweijährigen Übergangsfrist sind seit dem 25. Mai 2018 die Datenschutz-Grundverordnung (DSGVO) und parallel das neu gefasste Bundesdatenschutzgesetz (BDSG-neu) rechtsverbindlich. Damit werden Richtlinien zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht.

Das soll den Schutz personenbezogener Daten verbessern, einen freien Datenverkehr innerhalb der EU sicherstellen sowie den Datenschutz an die Herausforderungen durch Cloud Computing, Big Data, Soziale Medien oder Suchmaschinen anpassen.

Die DSGVO rückt allerdings nicht nur fragwürdige Datenpraktiken großer Internetkonzerne in den Fokus behördlicher Kontrolle, sondern auch alle Personendaten-relevanten Geschäftsprozesse kleiner und mittlerer Unternehmen. Das hat zahlreiche Konsequenzen und bürdet Planungsbüros ebenso wie Handwerksunternehmen viele Pflichten und zusätzliche Arbeit auf.

### Was sind Personendaten und wo fallen sie an?

Auch TGA-Planungsbüros, Gebäude-Energieberater und Handwerksbetriebe unterliegen nun strengeren Datenschutzregeln – denn auch sie erheben, speichern, verwalten, verarbeiten oder übermitteln personenbezogene Daten von Bauherren, Hauseigentümern, Projektpartnern, Handwerkern, Subunternehmern, Lieferanten, Dienstleistern und Mitarbeitern.

Deshalb müssen sich alle Inhaber planender oder ausführender Unternehmen mit datenschutzrechtlichen Fragen auseinandersetzen und den Personendatenschutz rechtskonform umsetzen. Im Fokus der DGSVO steht der Schutz personenbezogener Daten. Das sind prinzipiell alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Zu den personenbezogenen Daten gehören nicht nur Name, Anschrift und Telefonnummer, sondern auch E-Mail-Adressen, Bankdaten, Geburtsdaten, Berufsangaben oder auch IP-Adressen von Computern etc.

Da der Begriff der personenbezogenen Daten sehr weit gefasst ist, sind praktisch alle, während der Geschäftsabläufe von Planungsbüros und Handwerksbetriebenen anfallende personenbezogene Daten betroffen. Werden beispielsweise im Rahmen von Energieausweisen, Sanierungsplanungen, Kostenschätzungen oder Ausschreibungen Bauherren-, Hauseigentümer-, Fachingenieur- oder Handwerkerdaten verarbeitet, greift die DSGVO.

### Wann ist ein Einwilligung Betroffener erforderlich?

Allerdings ist nicht jeder Vorgang datenschutzrechtlich problematisch, denn die Personendatenverarbeitung ist immer dann zulässig, wenn unter anderem die Daten öffentlich zugänglich sind, betroffene Personen ihre Einwilligung gegeben haben, die Verarbeitung für die Erfüllung eines Vertrags, zur Durchführung vorvertraglicher Maßnahmen oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Bild: Sage

❷ **Praktisch jedes Unternehmen, das persönliche Daten verarbeitet, ist von der Datenschutz-Grundverordnung betroffen.**

Das bedeutet beispielsweise, dass energetische Analysen, Energieausweise oder Bauanträge eine besonderen Kunden-Einwilligung ebenso wenig voraussetzen, wie die (steuer-) rechtlich notwendige Archivierung von Projekt- und Kundendaten für einen Zeitraum von sechs oder zehn Jahren – eben weil sie zur für die Erfüllung eines Vertrags, respektive einer rechtlichen Verpflichtung erforderlich sind.

Auch für die Speicherung von Visitenkartendaten potenzieller Kunden oder Projektpartner ist keine Einwilligung der Betroffenen erforderlich, da sie der Geschäftsanbahnung dienen. Problematisch wird es, wenn diesen Personen ungefragt Newsletter oder Werbe-Mailings zugesandt werden, denn für jede Datennutzung, die nicht durch die DSGVO-Vorgaben erlaubt ist, muss eine möglichst schriftliche Einwilligungserklärung der Betroffenen eingeholt werden.

Oberstes Prinzip bei der Erhebung und Verarbeitung personenbezogener Daten ist die Datenminimierung. Das bedeutet, dass über eine Person nur jene personenbezogenen Daten gespeichert werden dürfen, die für die jeweilige Aufgabe zwingend erforderlich sind. Nicht zwingend erforderliche Daten sind zu löschen. Alle personenbezogenen Daten sind ferner vor Datenmissbrauch geschützt aufzubewahren. Sofern die jeweilige Software (Adressdatenbank, Lohnbuchhaltung, CRM, DMS etc.) dies zulässt, sollten personenbezogene Daten verschlüsselt werden.

## Verarbeitungsverzeichnis: Was wird wie wofür verarbeitet?

Da jedes Unternehmen Daten unterschiedlich verarbeitet, sind auch unterschiedliche Maßnahmen zu ergreifen. Zu den ersten Maßnahmen sollte deshalb eine Bestandsaufnahme und Dokumentation der internen Datenverarbeitungsprozesse gehören, die sämtliche personenrelevanten Unternehmensabläufe erfasst: Die Verarbeitung von Kundendaten (Adressen-, Vertrags-, Rechnungsdaten etc.), Personaldaten (Arbeitsverträge, die Erfassung Arbeitszeiten etc.) sowie entsprechende Daten von Planern, Handwerkern, Lieferanten, Subunternehmern, Dienstleistern und so weiter.

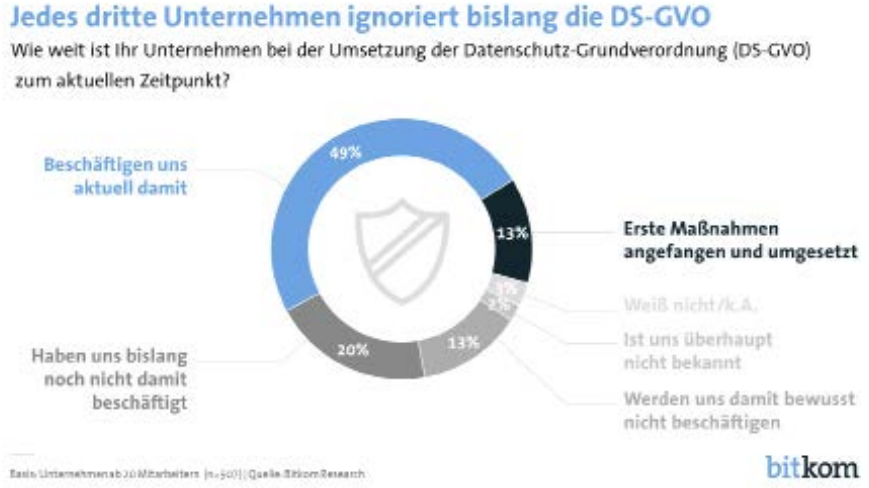


Bild: bitkom

❸ **Allerdings ignoriert Untersuchungen zufolge jedes dritte Unternehmen bislang die DSGVO-Vorgaben.**

In einem sogenannten Verarbeitungsverzeichnis muss dokumentiert werden, welche personenbezogenen Daten wie und wofür verarbeitet werden. Dabei sind alle Geschäftsabläufe zu berücksichtigen, in denen Personendaten verarbeitet werden. Erfasst werden unter anderem die Daten jener Mitarbeiter, die Personendaten verarbeiten, der Zweck der jeweiligen Datenverarbeitung, Kategorien betroffener Personen und Kategorien personenbezogener Daten, die Rechtsgrundlagen der Datenverarbeitung, Löschfristen, technische und organisatorische Datenschutzmaßnahmen etc.

Das Führen und regelmäßige Aktualisieren eines Verarbeitungsverzeichnisses ist Pflicht und dient als Nachweis für die Rechtmäßigkeit der Datenverarbeitung, respektive als Entscheidungsgrundlage, ob ein Anpassungsbedarf besteht: Ist die Verarbeitung gemäß den DSGVO-Vorgaben erforderlich und zulässig? Bedarf es einer Einwilligung Betroffener? Wer hat Zugriff auf die Daten? Wurden alle notwendigen Maßnahmen zur Datensicherheit getroffen? Birgt die Verarbeitung Risiken für die Betroffenen? Falls ja, ist gegebenenfalls eine sogenannte Datenschutz-Folgenabschätzung erforderlich? Welche weiteren Pflichten entstehen? Je nach Komplexität der Datenverarbeitungsprozesse kann für die Beantwortung dieser und weiterer Fragen die Unterstützung externer Berater sinnvoll sein.

## Welche sonstigen Pflichten sind zu beachten?

Unternehmen werden mit der DSGVO zahlreiche weitere Pflichten auferlegt, die im Folgenden nur beispielhaft genannt werden können:

**Auftragsverarbeitungsvertrag:** Wird ein externer Dienstleister damit beauftragt, personenbezogene Daten zu verarbeiten – das trifft praktisch auf alle Anbieter von Cloud-Diensten zu (Webhoster, Projekträume, Anbieter von E-Mail- oder Messenger-Diensten, aber auch von webbasierter ERP-Branchensoftware, Büro- und Projektmanagementsoftware, Zeiterfassung etc.) – muss mit diesem ein sogenannter Auftragsverarbeitungsvertrag abgeschlossen werden. Darin verpflichtet er sich, die Vorgaben der DSGVO einzuhalten. Anbieter entsprechender Dienste halten auf ihren Webseiten meist entsprechende Formulare zum Download bereit.

**Technische und organisatorische Maßnahmen:** Je nach individueller Risikobewertung sind Betriebe verpflichtet, „technische und organisatorische Maßnahmen" zu ergreifen, um Personendaten wirksam zu schützen. Das können Passwörter, Datenverschlüsselungen, Löschfristen oder Maßnahmen zum Viren-, Diebstahl- oder Einbruchschutz sein. Da Mitarbeiter im Hinblick auf den Datenschutz häufig ein Schwachpunkt sind, sind auch Unterweisungen und Vereinbarungen zur Nutzung und Übermittlung von Kun-



: Hier bietet das TGAepaper (WEBCODE 595030) zusätzliche Infos und Funktionen an.

dendaten sowie zum konsequenten Einsatz von Passwörtern und anderen Schutzmaßnahmen am Arbeitsplatz sinnvoll. Die Datenverarbeitung über einen externen Dienstleister abzuwickeln, kann Unternehmen von diesen Pflichten befreien, allerdings müssen ein DSGVO-konformer Dienstleister sorgsam ausgewählt und mit diesem detaillierte Auftragsverarbeitungsverträge abgeschlossen werden.

**Informationspflichten:** Ein elementarer DSGVO-Grundsatz ist Transparenz. Betroffene sollen künftig besser in der Lage sein, eine Erhebung, Verarbeitung oder Nutzung ihrer Daten zu überprüfen. Daraus ergeben sich weitreichende Informationspflichten gegenüber den Betroffenen, zum Beispiel Kunden, Bauherren oder Mitarbeitern. Unternehmen müssen auf Anfrage Auskunft geben können, unter anderem über Verantwortliche und Zwecke der Datenverarbeitung, Dauer der Datenspeicherung, gegebenenfalls eine Weiterleitung an Dritte etc. Betroffene müssen auf ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch gegen die Verarbeitung sowie eine Datenübertragbarkeit hingewiesen werden. Eventuelle Datenpannen sind innerhalb von 72 Stunden beim jeweiligen Landesdatenschutzbeauftragten sowie den Betroffenen zu melden.

**Datenschutzbeauftragter:** Ob ein Unternehmen einen betrieblichen Datenschutzbeauftragter bestellen muss, hängt davon ab, ob im Unternehmen mindestens zehn Personen regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Hat ein Unternehmen mindestens zehn Mitarbeiter und sind diese beispielsweise über den täglichen Umgang mit E-Mails, Aufträgen oder Projekten mit der regelmäßigen Bearbeitung personenbezogener Daten beschäftigt, ist ein betrieblicher Datenschutzbeauftragter Pflicht. Er kümmert sich um die Einhaltung der Vorgaben und überwacht das vorgesehene Schutzniveau. Wird er intern bestellt, muss er entsprechend ausgebildet und für seine Aufgaben freigestellt werden. Außerdem genießt er einen besonderen Kündigungsschutz.

### Kein Grund zur Panik, aber sicher ist sicher …

Zwei Jahre lang hat sie keiner beachtet – und jetzt bricht die Panik aus. Während der zweijährigen Übergangsfrist hatte sich kaum jemand für die DSGVO interessiert. Erst kurz vor dem Stichdatum stieg die Fieberkurve und bei vielen Unternehmen existieren noch Umsetzungslücken. Weil eine Umsetzung der Vorgaben von heute auf morgen nicht möglich ist, sollte man – gegebenenfalls mit externer Expertenhilfe – zumindest ein Konzept erarbeiten, anhand dessen sich der Personendatenschutz im Unternehmen schrittweise umsetzen lässt. Schließlich drohen bei Verstößen bis zu 4 % des Jahresumsatzes eines Unternehmens oder 20 Mio. Euro sowie Schadensersatzansprüche.

Bild: STRATO AG

**❹ Deutsche Anbieter orientieren sich zwar den strengen hiesigen Datenschutzregeln – dennoch ist bei der Nutzung von Online-Diensten stets ein Auftragsverarbeitungsvertrag erforderlich.**

Vermutlich wird aber auch die DSGVO nicht so heiß gegessen, wie sie jetzt teilweise von einer Datenschutzdienstleister-Lobby hochgekocht wird. Schließlich haben allzu streng ausgelegte DSGVO-Vorgaben das Potenzial, EU-weit den Online-Datenverkehr und den Austausch digitaler Daten erheblich zu behindern. Damit würde die DSGVO einem ihrer Ziele – der Förderung eines freien EU-Datenverkehrs – zuwiderlaufen.

In erster Linie werden wohl personendatensensible Unternehmen und Berufsgruppen von Datenschützern unter die Lupe genommen: Anbieter von Suchmaschinen, Social-Media- und anderen Cloud-Diensten, aber auch Krankenkassen, Arztpraxen, Apotheken, Rechtsanwaltskanzleien etc. Heikel für alle könnten mögliche Abmahnwellen gegen die Internetauftritte von Unternehmen werden, weil sie öffentlich sind. Deshalb sollte jeder kommerzielle Webseitenbetreiber seine Seiten vorsichtshalber auf mögliche Problembereiche durchforsten und gegebenenfalls an die neuen Vorgaben anpassen.

**Marian Behaneck**

### Quellen und weitere Infos

[1] www.dsgvo-gesetz.de DSGVO- und BDSG-neu-Text
[2] www.datenschutzbeauftragter-info.de Informationen zum Datenschutz
[3] www.datenschutz-grundverordnung.eu Infos, Schulungen, Kommentare
[4] www.heise.de siehe: „Topthemen DSGVO“
[5] www.bitkom.de Suche: „DSGVO“
[6] www.wikipedia.de Suche: „DSGVO“

## DSGVO-Tipps

- **Ruhe bewahren! Alle DSGVO-Vorgaben lassen sich ohnehin nicht von heute auf morgen, sondern nur in einem kontinuierlichen Prozess sukzessive umsetzen.**
- **Da die DSGVO-Vorgaben nicht von heute auf morgen umsetzbar sind, sollte zunächst ein Zeitplan ausgearbeitet werden, der die schrittweise Umsetzung der Datenschutzvorgaben zum Ziel hat.**
- **Zu den ersten Maßnahmen sollte eine Bestandsaufnahme und Dokumentation der internen Datenverarbeitungsprozesse gehören, die sämtliche personenrelevanten Unternehmensabläufe erfasst.**
- **In einem sogenannten Verarbeitungsverzeichnis sollte anschließend dokumentiert werden, welche personenbezogenen Daten wie und wofür verarbeitet werden.**
- **Um möglichen Abmahnungen vorzubeugen, sollte man die Unternehmens-Webseiten auf DSGVO-Konformität prüfen und Problembereiche anpassen:**

**Achtung Webseitenbetreiber!**

**Auch Betreiber von Unternehmens-Webseiten sind von der DSGVO betroffen. Relevant sind bereits die Wahl des Webhosters, die Verwendung von Cookies oder Analysesoftware, mit denen individuelle Aktivitäten von Besuchern dokumentiert und analysiert werden können. Die Verwendung von Kundenzitaten oder Referenzadressen ist ebenso zustimmungspflichtig wie der Einsatz von Social-Media-Plug-Ins. Für kommerzielle Webseiten ist ferner eine rechtskonforme Datenschutzerklärung Pflicht. Online-Generatoren helfen bei der individuellen Zusammenstellung (z. B.: dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de). Weitere Auflagen ergeben sich aus der DSGVO-Verpflichtung zur Datenminimierung, Integrität und Vertraulichkeit. So müssen etwa Kontaktformular-Daten verschlüsselt übertragen werden.**