Verbandsrundschreiben
22. Jahrgang / Sonderheft DS-GV / 2018

Datenschutz-Grundverordnung (DS-GVO) 25. Mai 2018

Wenn am 25. Mai 2018 die neue Datenschutz-Grundverordnung in Kraft tritt, drohen Unternehmen hohe Strafen. Wie Sie sich jetzt vorbereiten – eine der vielen DSGVO-Checkliste.

Am 25. Mai tritt die neue Datenschutz-Grundverordnung (DSGVO) in Kraft, die Unternehmer zwingen soll, persönliche Daten von Kunden und Mitarbeitern besser zu schützen. Seither hängt dieses Gesetzesungetüm (99 Artikel) wie ein Damoklesschwert über vielen Unternehmen. Denn erstens ist für Nicht-Juristen (und auch für einige Juristen) kaum zu durchschauen, was nun eigentlich zu tun ist. Und zweitens sind die Strafen, die im Raum stehen, gepfeffert.
Mit der Checkliste, die wir mit Unterstützung des Bundesverbandes Digitale Wirtschaft (BVDW) erstellt haben, sind Sie vorbereitet.

1. Datenschutzbeauftragten benennen, wenn nötig

Unternehmen müssen unter bestimmten Voraussetzungen einen Datenschutzbeauftragten benennen. Er ist Pflicht, wenn im Unternehmen personenbezogene Daten automatisiert verarbeitet werden, also per EDV.

Personenbezogene Daten sind insbesondere Kundendaten und Mitarbeiterdaten.

Ausnahme: Für kleine Betriebe macht die Verordnung eine Ausnahme: Sind regelmäßig nur neun oder weniger Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt, braucht ein Unternehmen KEINEN Datenschutzbeauftragten.
Dann kann der Geschäftsführer selbst den Datenschutz übernehmen.

Achtung: Es sind auch jene Mitarbeiter zu berücksichtigen, die nur ab und an Daten verarbeiten, etwa Zugriff auf die Kundendatenbank haben. Es spielt keine Rolle, ob ein Mitarbeiter Teil- oder Vollzeit arbeitet, freier oder fester Mitarbeiter ist, Praktikant oder Auszubildender. Entscheidend ist die Anzahl der Köpfe.

Wann die Ausnahme nicht gilt: Das Unternehmen verarbeitet Daten, für die eine Datenschutz-Folgenabschätzung nötig ist. Das ist bei allen Daten der Fall, bei denen ein hohes Risiko für die Betroffenen besteht, etwa bei Daten zu ihrer ethnischen Herkunft, sexuellen Orientierung, Gesundheit oder zur politischen Einstellung. Auch eine kleine psychotherapeutische Praxis, die solche Daten in der Patientenakte speichert, braucht also einen Datenschutzbeauftragten.

Achtung:
bei Kreditvermittlungen für Brennstofflieferungen, Abfragen über Wirtschaftsauskünfte!

Was muss der Datenschutzbeauftrage können?
Die Fachkunde des Datenschutzbeauftragten muss sichergestellt sein, etwa durch Fortbildungen bei der Industrie- und Handelskammer.

2. „Verzeichnis der Verarbeitungstätigkeiten" anlegen

Jedes Unternehmen muss ein sogenanntes „Verzeichnis der Verarbeitungstätigkeiten" anlegen (dies ergibt sich aus Art. 30 der DSGVO).
In der Tabelle listet man auf, welche Daten wann, wie und warum im Unternehmen erhoben werden. Etwa die Daten seiner Kunden: Name, Adresse, Telefonnummer.

Achtung: Hier nicht die internen Daten vergessen, die verarbeitet werden, etwa Personaldaten, Daten aus der Lohnbuchhaltung und so weiter.

Bei größeren Unternehmen sollte ein Projektverantwortlicher ernannt werden, der alle Mitarbeiter, die Datenverarbeitung verantworten (und eventuell auch Lieferanten und Partner) befragt.

Abgefragt werden sollte:

- Welche Informationen erhalten Betroffene (zum Beispiel die Kunden) über die Erhebung und Speicherung personenbezogener Daten?
- Wie werden diese Informationen erteilt: Stehen Sie zum Beispiel in den AGB, in einem Text neben einer Checkbox auf der Website oder teil man sie mündlich mit?
- Welche Daten werden erhoben, welchem Zweck dient die Datenerhebung, wie werden diese Daten weiterverarbeitet?
- Daraus leitet sich ab, ob es eine gesetzliche Erlaubnis gibt, die Daten zu verarbeiten – etwa bei einer Vertragsbeziehung – oder ob der Betroffene der Datenverarbeitung erst zustimmen muss.
- Werden Daten anonymisiert oder pseudonymisiert?
- Wie lange werden die Daten gespeichert?
- Werden die Daten weitergegeben? Wenn ja, an wen? Ist dieser ebenfalls für den Datenschutz verantwortlich?
- Wo werden die Daten gespeichert? Werden sie außerhalb der EU gespeichert? Falls ja: Sind die Voraussetzungen zur Übermittlung in Drittstaaten erfüllt?
- Werden die Daten ausreichend durch technische und organisatorische Maßnahmen geschützt?

Daraus erstellt man dann ein Verarbeitungsverzeichnis.

Bei einem Brennstoffhändler könnte das Verarbeitungsverzeichnis zum Beispiel so aussehen:

1. Kundenstammdaten

Verantwortlich Brennstoffhandel Brikett, Adresse, Telefonnummer
Zweck Terminabsprache, Brennstofflieferung
Betroffene Kunden des Brennstoffhandel Brikett
Wer kann auf die Daten zugreifen?
Alle Mitarbeiter des Brennstoffhandel Brikett
Datenkategorie Kundenstammdaten (Name, Telefonnummer, E-Mail-Adresse)
Brennstoffe Holz, Kohle Pellet, Heizöl, DK…usw…..

Übermittlung an Drittstaaten: Nein
Löschfrist Bei Widerruf des Betroffenen
(Aufbewahrungsfristen Finanzbehörden)
Rechtsgrundlage DSGVO Art. 6, Abs. 1b
Einwilligung des Betroffenen
Jeder Kunde wird auf die Erfassung der Daten durch die Mitarbeiter mündlich hingewiesen und darauf aufmerksam gemacht, dass er diese Daten jederzeit einsehen und löschen lassen kann.

2. Bewerberdaten

Verantwortlich Brennstoffhandel Brikett, Inhaber Kohle, Adresse, Telefonnummer
Zweck Bewerbermanagement
Betroffene Bewerber
Wer kann auf die Daten zugreifen? Inhaber und Geschäftsführer Kohle
Datenkategorie Bewerbungsmappen, Lebensläufe, Adressdaten (Name, Adresse, Telefonnummer, E-Mail-Adresse)
Übermittlung an Drittstaaten Nein
Löschfrist Sechs Monate nach Beendigung des Bewerbungsverfahrens
Rechtsgrundlage Art. 13 Abs. 1 und Abs. 2 DSGVO
Einwilligung des Betroffenen Bewerber werden mit einer automatischen E-Mail über den Zweck der Datenerhebung und die Dauer der Datenaufbewahrung informiert.
Die Unternehmen müssen darüber hinaus den Weg der Daten nachzeichnen, von der Erhebung (etwa bei einer Online/Telefonische-Terminvergabe der Lieferung) über die Speicherung (etwa bei einem externen Anbieter für Terminmanagement) bis hin zur Nutzung (zum Beispiel durch die Mitarbeiter).

Ein solches Verzeichnis ist übrigens schon nach dem alten Bundesdatenschutzgesetz verpflichtend, die wenigsten haben es aber bis jetzt geführt.

3. Prozesse festlegen und Prozesshandbuch schreiben

Unternehmer sollten jetzt alle mit Datenverarbeitung verbundenen Prozesse dokumentieren und – wenn nötig – optimieren. Zum Beispiel:

- Wie werden Kunden über die Verarbeitung ihrer Daten informiert?
- Wie reagieren Mitarbeiter, wenn Kunden fragen, welche Daten von ihnen gespeichert wurden?
- Was ist der Prozess, wenn ein Kunde darauf besteht, dass seine Daten gelöscht werden? Wer ist dafür verantwortlich?
- Was ist der Prozess, falls es zu einem Datenleck kommt und personenbezogene Daten in falsche Hände geraten?
- Denn Achtung: Kommen die Daten abhanden, zum Beispiel durch einen Hackerangriff, müssen Unternehmen binnen 72 Stunden die zuständige Landesdatenschutzbehörde informieren.
- Ist das Ziel, warum Daten gespeichert wurden, erreicht, müssen die Daten gelöscht werden (Bei einem Gewinnspiel etwa nach der Ermittlung der Gewinner). Wie ist der Löschprozess organisiert?
- Wie werden Mitarbeiter geschult, damit sie diese Prozesse kennen und ausführen können?

4. Datenschutz-Folgeabschätzung durchführen, wenn nötig

Empfehlung bei Kreditvermittlungen für Brennstofflieferungen

Wer mit besonders sensiblen Daten arbeitet – etwa Arztpraxen oder Versicherungsmakler – muss damit besonders umsichtig umgehen und unter Umständen eine so genannte Datenschutz-Folgeabschätzung durchführen. Das gilt für alle Unternehmen, die eine Identifizierung und Kategorisierung der Person ermöglichen nach Themen wie zum Beispiel Sexualität, Krankheiten, Finanzen, rassische oder ethnische Herkunft oder politischen Ansichten – denn hier besteht ein besonders hohes Risiko für die Betroffenen, wenn diese Daten missbraucht werden.
Eigentlich sollen die Datenschutzbehörden eine Liste herausgeben, die besagt, welche Datenverarbeitungsvorgänge eine Datenschutz-Folgeabschätzung voraussetzen.

Diese Liste gibt es aber bisher nicht, sodass im Einzelfall entschieden werden muss. Ein hohes Risiko kann sich aus der Art der Daten, ihrem Umfang oder dem Zweck der Datenverarbeitung ergeben.

Ziel der Datenschutz-Folgeabschätzung ist, die Risiken für die Persönlichkeitsrechte der betroffenen Personen zu kennen, um so geeignete Schutzmaßnahmen treffen zu können.

Worin besteht eine Datenschutz-Folgeabschätzung?

- Beschreibung der Datenverarbeitungsvorgänge.
- Beschreibung des Zwecks der Datenverarbeitung und Begründung, warum das Unternehmen ein berechtigtes Interesse daran hat. Die Datenverarbeitung muss im Hinblick auf den Zweck verhältnismäßig sein.
- Beschreibung der Risiken, die für betroffene Personen bestehen.
- Dokumentation: Was wird technisch und organisatorisch getan, um diese Daten gegen unberechtigten Zugriff oder Weitergabe zu sichern?
- Dokumentation: Wie wird im Falle eines Leaks (undichte Stelle in der DV) verfahren?
- Dokumentation: Welche Kontrollmechanismen greifen, damit die Daten geschützt bleiben?

Wichtig: Die Landesdatenschutzbehörden haben hier übrigens eine beratende Funktion.

5. Alle Anstrengungen dokumentieren

Unternehmer sollten alle ihre Anstrengungen dokumentieren:
Zu welchem Seminar ist der Datenschutzbeauftragte gegangen?
Welche Firewall wurde wann installiert?
Welche Verträge wurden mit Dienstleistern geschlossen?
Denn selbst bei Datenlecks oder Verstößen wie Fehlern in der Datenschutz-Erklärung besteht bei guter Dokumentation die Chance, ohne Bußgeld davonzukommen.
Dafür muss man aber die Unterlagen auf Anfrage umgehend vorlegen können.

Datenschutz-Grundverordnung erste Schritte für Unternehmen

Die Datenschutzgrundverordnung DSGVO mit ihren Nachweispflichten gilt ab dem 25. Mai 2018. Im Fall einer Datenschutz-Kontrolle wird eine typische erste Frage sein:
Wo ist die Dokumentation, wie das Unternehmen personenbezogene Daten verarbeitet, welche Rechtsgrundlage besteht für jede einzelne Verarbeitung?
Dann ist es wichtig, dass das Unternehmen ein „Verzeichnis von Verarbeitungstätigkeiten" im Sinne des Art. 30 DSGVO vorlegen kann, und zu jeder Verarbeitung eine Rechtsgrundlage nennen kann.
Art. 6 Abs. 1 DSGVO listet die Rechtsgrundlagen systematisch auf, säuberlich sortiert in Buchstabe a bis f.

a) Wirksame und nachweisbare Einwilligung der betroffenen Person (freiwillig und informiert erteilt, jederzeit widerruflich)
b) erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen
c) erforderlich zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt
d) erforderlich, um lebenswichtige Interessen der betroffenen oder einer anderen Person zu schützen
e) erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde
f) erforderlich zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen

Ordner anlegen

1. **Angestellte belehren und Belehrung dokumentieren- abheften**
   a. **Anhang 2** – Muster für ein Informationsblatt zur Verarbeitung von Beschäftigtendaten
   b. **Anhang 5** – Muster für eine Verpflichtung auf das Datengeheimnis und Merkblatt

2. Information der Beschäftigten über den **Anhang 6 –** Prozessbeschreibung zu den Themen Auskunftsanspruch, Löschung, Berichtigung
   - Eventuell den unternehmerischen Bedürfnissen anpassen, falls keine eigene Personalabteilung existiert.

- Im Ordner unter Prozessbeschreibung abheften.

3. **Anlage 1** Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen entsprechend den betrieblichen Erfordernissen anpassen im Ordner abheften
4. **Anlage2** Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen kann als Muster dienen
5. **Anlage 3** Checkliste, Technische und organisatorische Maßnahmen abarbeiten und abheften.

Einige Hinweise im Umgang mit **Kundendaten**:
Nach der DS-GVO benötigen sie ab dem 25.05.2018 die datenschutzrechtliche Einwilligung der Kunden.

Anlagen:

Anlage A Praxis Datenschutz Anforderungen der datenschutzrechtlichen Einwilligung der Kunden

Anlage B Praxis Datenschutz Informationspflichten bei Erhebung personenbezogener Daten

Anlage C Auskunftserteilung eines Brennstoff- und Mineralölhandels / Energiehändler an einen Kunden

---

Die Datenschutzkonferenz (DSK) veröffentlicht seit Juli 2017 Auslegungshilfen zur Datenschutz-Grundverordnung (DS-GVO). In diesen Kurzpapieren werden unter den deutschen Aufsichtsbehörden abgestimmte einheitliche Sichtweisen zu verschiedenen Kernthemen der DS-GVO wiedergegeben. Die in den Papieren enthaltenen Auffassungen stehen unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung durch den Europäischen Datenschutzausschuss.

Die Kurzpapiere des BayLDA, die bereits seit Juni 2016 in regelmäßigen Abständen erschienen sind, können ebenso heruntergeladen werden.

https://www.lda.bayern.de/de/datenschutz_eu.html

Anwaltlicher Telefonservice des SBMV mit der HAGER Partnerschaft Rechtsanwälte

Der SBMV bietet auch im Jahre 2018 einen anwaltlichen Telefonservice für seine Mitglieder an. Soweit Mitglieder des SBMV Fragen zu Rechtsproblemen haben, so sollen diese Fragen direkt fernmündlich oder aber auch schriftlich gerichtet werden können an die Partnerschaft. Von dort erfolgt dann eine entsprechende Beantwortung bzw. Beratung. Die Auskünfte bzw. die Beratung der Mitglieder zu Rechtsfragen durch die Partnerschaft erfolgt fernmündlich, im Bedarfsfalle aber auch persönlich in den Kanzleiräumen der Partnerschaft.
Vornehmlicher Ansprechpartner bei der Partnerschaft ist:
Herr Rechtsanwalt Mirko Zebisch
Tel.: 0341/ 30 931-73; E-Mail: zebisch@hager-partnerschaft.de

Datenschutzrecht: Rechtsanwalt Dr. Andreas Friedrich
HAGER Rechtsanwälte PartG mbB
Floßplatz 4, 04107 Leipzig
Tel: 0341 / 30 931 75
Fax: 0341 / 30 931 99
friedrich@hager-partnerschaft.de
www.hager-partnerschaft.de

Diese Zusammenfassung erhebt keinen Anspruch auf Vollständigkeit.

Jegliche Haftung wird ausgeschlossen.

Folgende Quellen wurden zur Erarbeitung herangezogen:

Impulse Medien GmbH , https://www.impulse.de

Materialien von RA Sabine Link, Externe Datenschutzbeauftragte und Unternehmensberatung Schulte-Marxloh-Str. 19, 47169 Duisburg
Telefon: 0176-84 88 50 82 oder 0203-34 98 30 45
Email: info@datenschutz-link.de, Internet: www.datenschutz-link.de

Redaktionsschluss: 03.04.2018	Für den Inhalt wird keine Haftung übernommen.	Herausgeber: SBMV e. V. www.sbmv.de	© SBMV Service und Marketing GmbH
Redaktion: Joachim Laue	✆ (03 42 04) 35 11 32 🖷 (03 42 04) 70 71 20 (01 77) 2 78 80 50 joachim.laue@sbmv.de	Vorsitzender: Andreas Lorenz Geschäftsführer: Joachim Laue	Geschäftsstelle: Papitzer Straße 9 04435 Schkeuditz