Dickemann-Weber GmbH & Co. KG
Friedhofsweg 1
76872 Erlenbach b. Kandel
Tel: +49 (0)72 75 / 729 81-0
Fax: +49 (0)72 75 / 729 81-50
E-Mail: info@dickemann-weber.com

EU-Datenschutz-Grundverordnung (DSGVO)

Hinweis: *Dies ist eine Zusammenfassung der DSGVO als Ergänzung zu unserer Fachliteratur für Weiterbildungen der IHK. Der Verfasser übernimmt keine Haftung und Verantwortung für Vollständigkeit und Richtigkeit der gemachten Angaben.*

Die EU-Datenschutz-Grundverordnung (DSGVO) bringt zahlreiche Neuerungen für den Datenschutz im Unternehmen mit sich.

Ab **25. Mai 2018** gilt in Deutschland die **Datenschutzgrundverordnung** (DSGVO) der Europäischen Union (EU).

Zeitgleich tritt ein dazu gehöriges Bundesdatenschutzgesetz neuer Fassung (**BDSG neu**) in Kraft, das die bisherigen datenschutzrechtlichen Vorschriften (BDSG alte Fassung) ersetzt.

Ziel der DSGVO:

Ein weitestgehend **einheitliches Datenschutzrecht innerhalb der EU.**
Mit der DSGVO wird das Datenschutzrecht innerhalb Europas vereinfacht, um dem Einzelnen mehr Kontrolle über seine Daten zu verschaffen.

Grundsätze des Datenschutzes:

Art. 5 Abs. 1 DSGVO zählt die Grundsätze auf, die für die gesamte Datenverarbeitung gelten:

- **Rechtmäßigkeit der Verarbeitung**:
  Daten dürfen nur verarbeitet werden, wenn es dies entweder gesetzlich erlaubt ist, oder eine wirksame Einwilligung des „Betroffenen“ vorliegt.
- **Verarbeitung nach Treu und Glauben**:
  Bei dem Grundsatz von Treu und Glauben handelt es sich um einen unbestimmten Rechtsbegriff und die Frage ob ein Verhalten als redlich bzw. anständig anzusehen ist.
  Besteht ein „berechtigtes Interesse“ an einer Datenverarbeitung?

- **Transparenz**:
  Die betroffene Person muss erkennen und wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z.B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht)
- **Zweckbindung**:
  Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Und die Zwecke der Datenverarbeitung müssen grds. bereits bei der Erhebung der Daten eindeutig festgelegt sein.
  Es dürfen keine Daten auf Vorrat erhoben werden.
- **Datenminimierung**:
  Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung notwendig sind. Die Daten müssen insbesondere auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.
- **Richtigkeit der Datenverarbeitung**:
  Die Daten müssen sachlich richtig sein, anderenfalls müssen sie berichtigt oder gelöscht werden.
- **Speicherbegrenzung**:
  (vgl. Art. 17 DSGVO, „Recht des Nutzers auf Vergessenwerden“, Datensparsamkeit)
  Wann werden Daten nicht mehr benötigt und können daher gelöscht werden (->Pflichten zur Löschung von Daten)?
  Zudem: Nutzung der Möglichkeiten zur Anonymisierung von Daten.
- **Integrität und Vertraulichkeit**:
  (vgl. Art. 32 DSGVO: Sicherheit der Daten)
  Personenbezogene Daten müssen so verarbeitet werden, dass Ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist.
- **Rechenschaftspflicht:**
  Führen eines Verzeichnisses der Verarbeitungstätigkeiten durch die verantwortliche Stelle, also das Unternehmen oder die Institution, gem. Art. 5 Abs. 2 DSGVO.
  Die Verantwortliche müssen nicht nur all ihre Datenverarbeitungstätigkeiten, sondern auch die Maßnahmen dokumentieren, die sie zur Einhaltung der Anforderungen der DSGVO getroffen haben.

Rechtmäßigkeit der Verarbeitung personenbezogener Daten:

Grundsatz:

Die Verarbeitung von personenbezogenen Daten ist **grundsätzlich verboten**.

Ausnahme:

Eine Datenverarbeitung ist zulässig, wenn

1. eine gesetzliche Vorschrift sie erlaubt

a) § 26 Abs.1 S.1 BDSG-neu enthält die gesetzliche Erlaubnis zum Zwecke des Beschäftigungsverhältnisses Daten zu verarbeiten, wenn es für die Entscheidung über die Begründung, Durchführung, Beendigung oder Ausführung des Arbeitsverhältnisses erforderlich ist.

Hinweis:

Dies entspricht weitestgehend dem alten § 32 Abs.1 S.1 BDSG.

Weitere Erlaubnistatbestände nach § 26 Abs.1 BDSG sind:

Erforderlichkeit zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten, § 26 Abs.1 S.1 BDSG-neu.

Verarbeitung personenbezogene Daten für Zwecke der Aufdeckung von Straftaten unter bestimmten Voraussetzungen, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips, § 26 Abs.1 S.2 BDSG-neu.

Hinweis: Dies deckt sich mit dem § 32 Abs. 1 Satz 2 BDSG-alt.

b) Daneben finden sich in Art. 6 DSGVO die allgemeinen gesetzlichen Erlaubnistatbestände.

Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig,

- wenn eine Einwilligung der betroffenen Person vorliegt, oder
- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen, oder
- zur Erfüllung einer rechtlichen Verpflichtung oder
- zum Schutze lebenswichtiger Interessen, oder
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder
- aufgrund einer Interessenabwägung erforderlich ist.

2. der Betroffene in die Datenverarbeitung einwilligt Art. 6 Abs.1 S.1 lit.a DSGVO und § 26 Abs.2 BDSG-neu

Die Einwilligung muss freiwillig, bestimmt, in informierter Weise, ausdrücklich und unmissverständlich erklärt werden.
Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DSGVO).

Die Einwilligung ist insbesondere dann freiwillig, wenn für den Beschäftigten ein wirtschaftlicher Vorteil erreicht wird oder der Arbeitgeber und der Beschäftigte gleichgelagerte Interessen verfolgen.

Die Einwilligung bedarf im Regelfall der Schriftform.

Der Beschäftigte ist darüber hinaus über die Zwecke der Datenverarbeitung und sein Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären.

Bei der Verarbeitung besonderer Arten personenbezogener Daten (u.a. Religion, sexuelle Neigung, Gesundheitsdaten) besteht zudem eine spezielle Hinweispflicht.

Hinweise:

- Im Grundsatz bleibt alles verboten, was nicht ausdrücklich erlaubt (Verbot mit Erlaubnisvorbehalt).
- Neue Definition des Beschäftigtenbegriffs in § 26 Abs.8 BDSG-neu:
  Im Vergleich zu der bisherigen Definition aus § 3 Abs. 11 BDSG-alt bezieht sich die Definition nunmehr ausdrücklich auch auf Leiharbeitnehmer im Verhältnis zum Entleiher; auf Freiwillige, die einen Dienst nach dem Bundesfreiwilligendienstgesetz leisten und auf Beamte des Bundes, Richter des Bundes, Soldaten und Zivildienstleistende.

Rechte der Betroffenen nach dem DSGVO und dem BDSG-neu

Folgende Rechte haben Betroffene nach dem DSGVO:

1. **Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person, Art. 13 DSGVO**
   Werden personenbezogene Daten bei der betroffenen Person erhoben, so muss der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten bestimmte Informationen mitteilen wie, Name und Kontaktdaten des verantwortlichen, Zwecke und Rechtsgrundlage der Datenverarbeitung, etc.
2. **Auskunftsrecht Art. 15 DSGVO, § 34 BDSG-neu und § 57 BDSG-neu**
   Betroffene haben das Recht, von der datenverarbeitenden Stelle eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind und verarbeitet werden. Falls Daten gespeichert werden, Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen.
3. **Recht auf Berichtigung Art 16 DSGVO und § 58 Abs.1 BDSG-neu**
   Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, haben die betroffenen Personen ein Recht auf Berichtigung. Der verantwortliche Datenverarbeiter muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.
4. **Recht auf Löschung Art. 17 DSGVO, § 35 BDSG-neu und § 58 Abs.2 BDSG-neu**
   Betroffene haben das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich geregelten Löschungsgründe vorliegt.
   Ein solcher Grund liegt vor, wenn
   - die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist,
   - die Daten unrechtmäßig verarbeitet wurden oder
   - der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat.
5. Recht auf Vergessenwerden Art 17 DSGVO
   Dies ist eine besondere Form des Löschungsanspruchs und bezieht sich auf Daten, die im world wide web veröffentlicht wurden. Die betroffene Person muss den Datenverarbeiter darüber informieren, dass sie die Löschung aller Daten, einschließlich sämtlicher Kopien und Links zu diesen Daten verlangt. Der Verantwortliche muss neben der Löschung zusätzlich alle Personen, die mit den jeweiligen Daten arbeiten, darüber informieren, dass die Daten zu löschen sind. Zu denken ist hier an erster Stelle an Suchmaschinen, die ebenfalls über den Löschungsantrag informiert werden müssen.

6. **Recht auf Einschränkung der Verarbeitung Art 18 DSGVO und § 58 Abs.3 BDSG-neu**
   Anspruch auf Sperrung der Daten, soweit Aufbewahrungsfristen oder unverhältnismäßig hoher Aufwand der Löschung entgegenstehen, oder die Richtigkeit der Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll.
7. **Recht auf Datenübertragbarkeit Art. 20 DSGVO**
   Betroffene haben den Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten.
8. **Widerspruchsrecht Art 21 DSGVO und § 36 BDSG-neu**
   Dem Betroffenen steht jederzeit ein Widerspruchsrecht gegen eine Datenverarbeitung zu.
9. **Recht auf Schadensersatz Art. 82 DSGVO und § 83 BDSG-neu**
   Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
10. **Anrufungsrecht des betrieblichen Datenschutzbeauftragten**
    Betroffene Personen können den Datenschutzbeauftragten zu allen Fragen zu Rate ziehen, die mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen. Der Datenschutzbeauftragte dient den betroffenen Personen somit als Ansprechpartner für sämtliche Fragen rund um den Datenschutz, Art. 38 Abs. 4 DSGVO.

Maßnahmen zur Datensicherheit nach dem BDSG

§ 64 Abs.1 BDGS-neu legt fest, dass **technische und organisatorische Maßnahmen** zu treffen sind, um die Ausführung dieses Gesetzes zu gewährleisten, also den Schutz der Daten sicherzustellen.

Nach § 64 Abs.2 BDSG-neu können solche Maßnahmen Pseudonymisierung und Verschlüsselung personenbezogener Daten sein.

Nach § 64 Abs.3 BDSG-neu sollen folgende Maßnahmen Datensicherheit gewährleisten:

Zugangskontrolle	Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Nur Befugte dürfen Zugang zu Datenverarbeitungssystemen erhalten. Gewährleistung z.B. durch Installation eines Zutrittssystems wie Ausweiskontrolle, Pförtner, elektronische Zutrittskontrollen
Datenträgerkontrolle	Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
Speicherkontrolle	Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
Benutzerkontrolle	Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte
Zugriffskontrolle	Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang

	haben. Gewährleistung z.B. durch Zugriff nur auf einzelne freigegebene Datenbereiche oder Datenfelder, Berechtigungskonzepte, Passwortregelungen, Kopierschutz, Zugriff nur von bestimmten Terminals aus, Schreib– und Löschschutzfunktionen
Übertragungskontrolle	Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
Eingabekontrolle	Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Gewährleistung z.B. durch automatische Nutzungsdokumentation, detailliertes Protokollierungssystem/Logdateien
Transportkontrolle	Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
Wiederherstellbarkeit	Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
Zuverlässigkeit	Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
Datenintegrität	Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
Auftragskontrolle	Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Gewährleistung z.B. durch stichprobenartige Kontrollen durch AG und Auftragnehmer, programmtechnische Sperren
Verfügbarkeitskontrolle	Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Gewährleistung durch Implementierung von Datensicherungskonzepten, z.B. regelmäßige Datensicherung nach festgelegtem Prinzip
Trennbarkeit	Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Gewährleistung z.B. durch funktionale Trennung des Datenbestandes, programmseitige Möglichkeit der Selektierbarkeit der Daten

Weitere Maßnahmen gewährleisten Datensicherheit:

Weitergabekontrolle	Daten dürfen bei ihrer Weitergabe nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Gewährleistung z.B. durch Datenübertragung in verschlüsselter Form, Protokollierung der Datenübermittlung, Zugang zu Speichermedien nur für Berechtigte
Organisationskontrolle	Die Mitarbeiter sind auf die Wahrung von Datengeheimnissen und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten.

	Gewährleistung z.B. durch Erarbeiten von Richtlinien und Dienstanweisungen, Instruktion der User, Verpflichtung auf den Datenschutz, stichpunktartige Kontrolle der User

Beauftragte für den Datenschutz

Der Datenschutzbeauftragte war bereits nach der alten Rechtslage eine zentrale Stelle für den Datenschutz. Seine Bedeutung nimmt durch die DSGVO und das BDSG-neu noch weiter zu.

Folgende Beauftragte für den Datenschutz werden unterschieden:

1. Datenschutzbeauftragte des **Bundes und der Länder, § 5 BDSG-neu**
2. **Betriebliche** Datenschutzbeauftragte, Art. 37 DSGVO und § 38 BDSG-neu

Sind Unternehmen verpflichtet einen Datenschutzbeauftragten zu bestellen?

Nach **Art. 37 DSGVO** müssen Unternehmen immer dann einen Datenschutzbeauftragten bestellen, wenn ihre Kerntätigkeit oder die des Auftragsverarbeiters

- aus Verarbeitungsvorgängen besteht, die nach Art, Umfang und/oder Zweck eine systematische Überwachung erfordern oder
- die Verarbeitung besonders sensibler Daten nach Art. 9 und 10 DSGVO betrifft.

§ 38 BDSG-neu erweitert die Gründe für die Benennung eines Datenschutzbeauftragten. Die Bestellung eines betrieblichen Datenschutzbeauftragten ist danach auch dann erforderlich, wenn das Unternehmen

- in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
- Verarbeitungen vornimmt, die der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO unterliegen (dies ist insbesondere relevant bei Gesundheitsdaten) oder
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet und zwar unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

Hinweise:

- Zu der Zahl der Personen zählen auch Teilzeitkräfte, Auszubildende, Leihpersonal sowie Geschäftsführer .

- Im Ergebnis führen diese erweiterten Voraussetzungen dazu, dass faktisch jedes mittlere oder größere Unternehmen in Deutschland einen Datenschutzbeauftragten bestellen muss.
- Jedes Unternehmen muss selbst klären, ob es einer Bestellpflicht unterliegt und einen Datenschutzbeauftragten bestellen muss.
- Nach Art. 38 DSGVO ist der Datenschutzbeauftragte frühzeitig einzubinden, fachlich weisungsfrei und berichtet unmittelbar der höchsten Managementebene.

Wer kann zum betrieblichen Datenschutzbeauftragten bestellt werden?

Gemäß Art. 37 Abs.5 DSGVO und § 5 BDSG-neu wird "der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DSGVO bzw. § 7 BDSG-neu genannten Aufgaben."

Zusammenfassung Voraussetzungen:

Zum betrieblichen Datenschutzbeauftragten können nach **Art. 37 Abs. 5 DSGVO und § 5 BDSG-neu** Personen bestellt werden, die folgende Voraussetzungen besitzen:

- Eine gewisse berufliche Qualifikation,
- Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis und
- die Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben (gem. Art. 39 DSGVO).

Hinweise:

- Konkrete Vorgaben hinsichtlich Kenntnissen oder Ausbildung sind jedoch weder in der DSGVO noch im BDSG-neu vorgesehen. Datenschutzbeauftragter kann daher grundsätzlich jeder werden.
- Die Bestellung eines Datenschutzbeauftragten muss nicht mehr schriftlich erfolgen. Aus Beweisgründen und zur Rechtsklarheit ist eine schriftlich verfasste Bestellungsurkunde aus der Beginn der Tätigkeit und die wahrzunehmenden Aufgaben hervorgehen, ratsam.
- Nicht bestellt werden darf eine Person, die in einen Interessenkonflikt geraten könnte oder für die eine Gefahr der Selbstkontrolle besteht, Art. 38 Abs.6 DSGVO.

Beachte:

Der betriebliche Datenschutzbeauftragte kann intern oder extern besetzt werden, Art. 37 Abs.6 DSGVO.

Vorteile eines externen Datenschutzbeauftragten:

- Die Unternehmen können ihre eigenen internen Ressourcen besser nutzen. Sie binden ihr Personal nicht mit diesen Aufgaben.
- Externe haben spezifisches Fachwissen, da sie auf Datenschutz spezialisiert sind.

Vorteile eines internen Datenschutzbeauftragten:

- Der interne Datenschutzbeauftragte kennt bereits die internen Unternehmensstrukturen und Abläufe.
- Die interne Lösung ist in den meisten Fällen für Unternehmen kostengünstiger als ein externer Datenschutzbeauftragter.

Welche wesentlichen Aufgaben und Tätigkeiten hat der betriebliche Datenschutzbeauftragte?

Die wesentlichen Aufgaben des betrieblichen Datenschutzbeauftragten werden in **Art. 39 DSGVO und § 7 BDSG-neu** genannt.

Zu ihnen zählen insbesondere folgende Aufgaben bzw. Pflichten:

- Unterrichtung und Beratung des Verantwortlichen bzw. Auftragsverarbeiters sowie deren Beschäftigten bezüglich ihrer datenschutzrechtlichen Rechten und Pflichten
- Überwachung der Einhaltung der Vorgaben der DSGVO
- Überwachung der Datenschutzstrategien einschließlich der Zuweisung von Zuständigkeiten
- Sensibilisierung und Schulung der relevanten Mitarbeiter
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung gem. Art. 35 DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle der Aufsichtsbehörde
- Risikobeurteilung
- Schaffung von Transparenz in der betrieblichen Datenverarbeitung
- Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
- Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Der Datenschutzbeauftragte ist im Rahmen seiner Aufgaben zur Geheimhaltung verpflichtet (-> Geheimhaltungspflicht, Verschwiegenheitspflicht) nach Art. 38 Abs.5 DSGVO
- Führen des Verarbeitungsverzeichnis (früher Verfahrensverzeichnis)
- Ansprechpartner für Geschäftsführung, Mitarbeiter in allen Fragen im Umgang mit Nutzer- und Kundendaten.

Hinweis:
Er kann im Unternehmen auch zusätzlich andere Aufgaben wahrnehmen, sofern sichergestellt ist, dass daraus keine Interessenkonflikte erwachsen nach Art. 38 Abs. 6 DSGVO.

Bsp. für Tätigkeitsfelder, welche zu einem Interessenkonflikt führen können:

- Mitglied der Unternehmensleitung
- Leitung der IT-Abteilung
- Leitung der Personal-Abteilung,
- Mitarbeiter der IT- oder Personal-Abteilung, wenn diese in der Lage sind, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen.

Wie können bzw. müssen die Unternehmen den betrieblichen Datenschutzbeauftragten unterstützen?

Der Datenschutzbeauftragte erhält durch die DSGVO eine wichtige organisatorische Stellung im Unternehmen.

Dem Verantwortlichen oder Auftragsverarbeiter drohen empfindliche Bußgelder, wenn der Datenschutzbeauftragte im Unternehmen seine Stellung nicht entsprechend der gesetzlichen Vorgaben ausüben kann.

Die Vorgaben zur Unterstützung des Datenschutzbeauftragten durch das Unternehmen umfassen insbesondere:

- **Vor- und Weiterbildung**,
  d.h., die Unternehmen müssen es dem Datenschutzbeauftragten ermöglichen, sein Fachwissen aufzubauen und aktuell zu halten (Kostenerstattungspflicht und Freistellungspflicht).
- **Ressourcen zur Aufgabenerfüllung**,
  d.h. die Unternehmen müssen dem Datenschutzbeauftragten ausreichend Ressourcen und Zeit zur Erfüllung aller seiner Aufgaben zur Verfügung stellen. Dem Datenschutzbeauftragten sind die erforderlichen Mittel, wie Hilfspersonal, Geräte u.ä., insbesondere auch eigene Räumlichkeiten zur Verfügung zu stellen.
- **Weisungsfreiheit**
  Bei der Ausführung seiner Aufgaben unterliegt der betriebliche Datenschutzbeauftragte keinen Weisungen, Artikel 38 Abs.3 S.1 DSGVO.
  Der Datenschutzbeauftragte ist der Geschäftsleitung disziplinarisch unmittelbar zu unterstellen und es ist ein direktes Vortragsrecht und eine direkte Vortragspflicht sicherzustellen (und Berichtspflicht)

- **Schutz des Datenschutzbeauftragten vor Benachteiligung**
  Unternehmen dürfen gemäß Art. 38 Abs. 3 DSGVO den Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligen.
- **Sonderkündigungsschutz des Datenschutzbeauftragten §§ 38 Abs. 2 in Verbindung mit 6 Abs. 4 BDSG-neu**
  Die Kündigung des Arbeitsverhältnisses des (internen) Datenschutzbeauftragten, dessen Benennung verpflichtend ist, ist nur unter den strengen Voraussetzungen des § 626 BGB zulässig (= besonderer Kündigungsschutz). D.h., die Kündigung eines Datenschutzbeauftragten ist unzulässig, es sei denn, es liegen Tatsachen vor, die für die Annahme eines wichtigen Grundes einer außerordentlichen Kündigung ausreichen.
  Dieser besondere Kündigungsschutz wirkt ein Jahr nach Abberufung des Datenschutzbeauftragten nach (= nachwirkender Sonderkündigungsschutz). Dieser zusätzliche Schutz stellt die Unabhängigkeit des Datenschutzbeauftragten gegenüber dem Unternehmen sicher.
- **Veröffentlichung von Kontaktdaten, Art. 37 Abs.7 DSGVO**
  Gemäß Art. 38 Abs. 4 DSGVO können betroffene Personen den Datenschutzbeauftragten wegen der Verarbeitung ihrer personenbezogenen Daten und der Wahrnehmung ihrer Rechte kontaktieren. Damit betroffene Personen dieses Recht ausüben können, müssen Unternehmen Kontaktdaten des Datenschutzbeauftragten veröffentlichen.
  Aber:
  - Veröffentlichung des Namens des DSB ist nicht zwingend erforderlich.
  - Eine unternehmensinterne Bekanntmachung genügt nicht.
- Zu den zu veröffentlichenden Kontaktdaten des Datenschutzbeauftragten gehören mindestens folgende Informationen:
  - Adresse
  - Telefon-Nummer und
  - E-Mail-Adresse des Datenschutzbeauftragten.
- Frühzeitige Beteiligung des Datenschutzbeauftragten
- Unterstützung des Datenschutzbeauftragten
- Vermeidung von Interessenkonflikten
- Die Unternehmen müssen sicherstellen, dass ihre Datenschutzbeauftragten keinen unvertretbaren Interessenkonflikten ausgesetzt sind, Art. 38 Abs.6 S.2 DSGVO.