



ITEBO
Unternehmensgruppe

Die neue EU-Datenschutzgrundverordnung –

Das müssen Sie wissen!



Ihr Ansprechpartner im Datenschutz

Holger Brinkmeyer

Holger Brinkmeyer (ass. iur.)
beschäftigt bei der ITEBO GmbH in
Osnabrück als

- Justiziar
- Externer Datenschutzbeauftragter

Arbeitsschwerpunkte

- Externer Datenschutz
- Vertragsrecht



ITEBO-Unternehmensgruppe

Unternehmensphilosophie

Full-Service-Anbieter von IT-Dienstleistungen

- von der Beratung
- über die Implementierung
- bis hin zum Betrieb komplexer Anwendungssysteme und IT-Infrastrukturen

Strategischer Partner, der die Sprache der Kunden spricht

- Gemeinden, Städte, Kreise und deren Tochterunternehmen
- Kirchen sowie kirchliche und soziale Einrichtungen
- Krankenhäuser
- Energieversorger
- Mittelständische Unternehmen

ITEBO-Unternehmensgruppe

Produkte & Services

Portfolio-Auszug

- SAP-Dienstleistungen – Von der SAP-Beratung bis zum SAP-Betrieb als zertifizierter SAP Hosting-Partner
- Personalmanagement – Vom Betrieb der Personalbuchhaltungssoftware bis zum ITEBO Payroll-Service
- E-Services – Dokumentenmanagementsystem, Realisierung von Internetauftritten (TYPO3), Softwareentwicklung
- Managed Services – Von der IT-Betreuung bis hin zum Betrieb der Serverinfrastruktur
- Outputmanagement – Vom Druck und Versand (mit Versandoptimierung) bis hin zum print as a service
- Datenschutz – Datenschutzbeauftragte und IT-Sicherheitsberatung

Ihre Ansprechpartner im Datenschutz

Servicebereich Datenschutz und IT-Sicherheit bei Itebo GmbH

- 7 Mitarbeiter mit unterschiedlichen Schwerpunkten
 - juristisch
 - IT / technisch
 - kaufmännisch

Arbeitsschwerpunkte

- Stellung des externen Datenschutzbeauftragten
- Datenschutzberatung
- IT-Sicherheitsberatung

Kundenschwerpunkt

- Öffentliche Auftraggeber
- Mittelständische Wirtschaftsunternehmen

Themenplan

1. Überblick EU-DSGVO

- **Aktueller Stand und Zeitplan**
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Aktueller Stand

Hintergrund und Zeitplan

- | Datenschutzgrundverordnung gilt **unmittelbar**, auch ohne dass sie in nationales Recht umgesetzt werden muss (Ausnahme: kirchliche Einrichtungen).
- | Die Datenschutzgrundverordnung (DSGVO) **gilt seit dem 25. Mai 2018**.
- | Relevant sind ebenfalls die **Erwägungsgründe**, die als Umsetzungshinweise angesehen werden können.
- | **Öffnungsklauseln** können für national weitergehende Regelungen genutzt werden, dürfen aber **nicht das Schutzniveau** senken.
- | Bestehende (**Datenschutz-**) **Gesetze gelten weiter**, dürfen der DSGVO aber nicht widersprechen (Keine Anwendung im Konfliktfall).

Aktueller Stand

Gesetzgebungsverfahren

Novellierung des BDSG:

- Datenschutz-Anpassungs- und -Umsetzungsgesetz EU, gilt seit dem 25. Mai 2018.
 - Relevant für alle öffentlichen Stellen des Bundes und alle nicht – öffentlichen Stellen (Unternehmen, Vereine)

Novellierung des NDSG:

- Niedersächsisches Datenschutzgesetz (NDSG),
 - Relevant für öffentliche Stellen des Landes und Kommunen in NDS

Novellierung katholische Datenschutzgesetzgebung

- Das katholische Datenschutzgesetz (KDG) löst die bisherige Anordnung über den Datenschutz (KDO) zum 24. Mai 2018 ab.
 - Relevant für alle Einrichtungen der katholischen Kirche

Novellierung evangelische Datenschutzgesetzgebung

- Das evangelische DSG-EKD in der Fassung von 1993 wird durch die neue Fassung des DSG-EKD zum 24. Mai 2018 abgelöst.
 - Relevant für alle Einrichtungen der evangelischen Kirche

Hinweise und Orientierungshilfen zum Thema EU-DSGVO

Homepage der Landesbeauftragten für Datenschutz Niedersachsen

- Auf der Homepage der LfD (www.lfd.niedersachsen.de) werden sukzessive unter der Rubrik „DSGVO“ die sog. „Kurzpapiere“ der DSK zu Schwerpunktthemen der DSGVO eingestellt.

Homepage der Gesellschaft für Datenschutz und Datensicherheit

- Auf der Homepage der Gesellschaft für Datenschutz und Datensicherheit (www.gdd.de) sind Praxishilfen zur DSGVO insbesondere mit Blickrichtung Wirtschaftsunternehmen eingestellt.

Homepage des Diözesandatenschutzbeauftragten der norddeutschen (Erz)-Bistümer

- Auf der Homepage des Diözesandatenschutzbeauftragten (www.datenschutz-kirche.de) finden sich in der Rubrik „KDG-Praxishilfen“ die Praxishilfen des Arbeitskreises der Diözesandatenschutzbeauftragten zu Schwerpunktthemen des KDG.

Hinweise und Orientierungshilfen zum Thema EU-DSGVO

| **Homepage zum Datenschutz in der evangelischen Kirche**

- Auf der Homepage zum Datenschutz der evangelischen Kirche (<https://datenschutz.ekd.de>) sind konkrete Vorlagen zur Umsetzung vorhanden, z.B. zu Verschwiegenheit, Videoüberwachung, Auftragsverarbeitung

| **Homepage des Bayrischen Landesbeauftragten für Datenschutz**

- Auf der Homepage des bayrischen Datenschutzbeauftragten (<https://www.lida.bayern.de>) sind Praxishilfen zur DSGVO für Vereine eingestellt.

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- **Neuerungen und deren Konsequenzen**
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Kernpunkte der DSGVO

Vergleich zu heute

Gestärkte **Betroffenenrechte**:

- NEU: Recht auf Vergessenwerden
- NEU: Recht auf Datenübertragbarkeit

Stärkere **Verpflichtung der Verantwortlichen** der Verarbeitung

Grundsätzliche **Rechenschaftspflicht**

- Nachweis einer ordnungsgemäßen Einwilligung
- Nachweisbarkeit der rechtmäßigen Verarbeitung

Datenschutz muss bereits **bei der Planung beachtet** werden:

- „privacy by design“ und „privacy by default“ als Grundsätze
- Datenschutz-Folgeabschätzung bei geplanter Verarbeitung sensibler Daten

Datenschutzbeauftragte bekommen verstärkte **Kontrollfunktion** und sind Hauptansprechpartner für die Aufsichtsbehörden.

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- **Was sind personenbezogene Daten?**
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Rechtmäßigkeit der Verarbeitung

**Die Verarbeitung
personenbezogener Daten ist
grundsätzlich verboten!**

Was sind personenbezogene

Daten?

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Beispiele:

- Allg. Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer,..)
- Kennnummern (Sozialversicherungsnummer, Steueridentifikationsnummer, Nummer bei der Krankenversicherung, Personalausweisnummer, Matrikelnummer,...)
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände,...)
- Online-Daten (IP-Adresse, Standortdaten,...)
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße,...)
- Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten,...)
- Kundendaten (Bestellungen, Adressdaten, Kontodaten usf.)
- Werturteile (Schul- und Arbeitszeugnisse,...)

Was sind besondere personenbezogene

Daten?

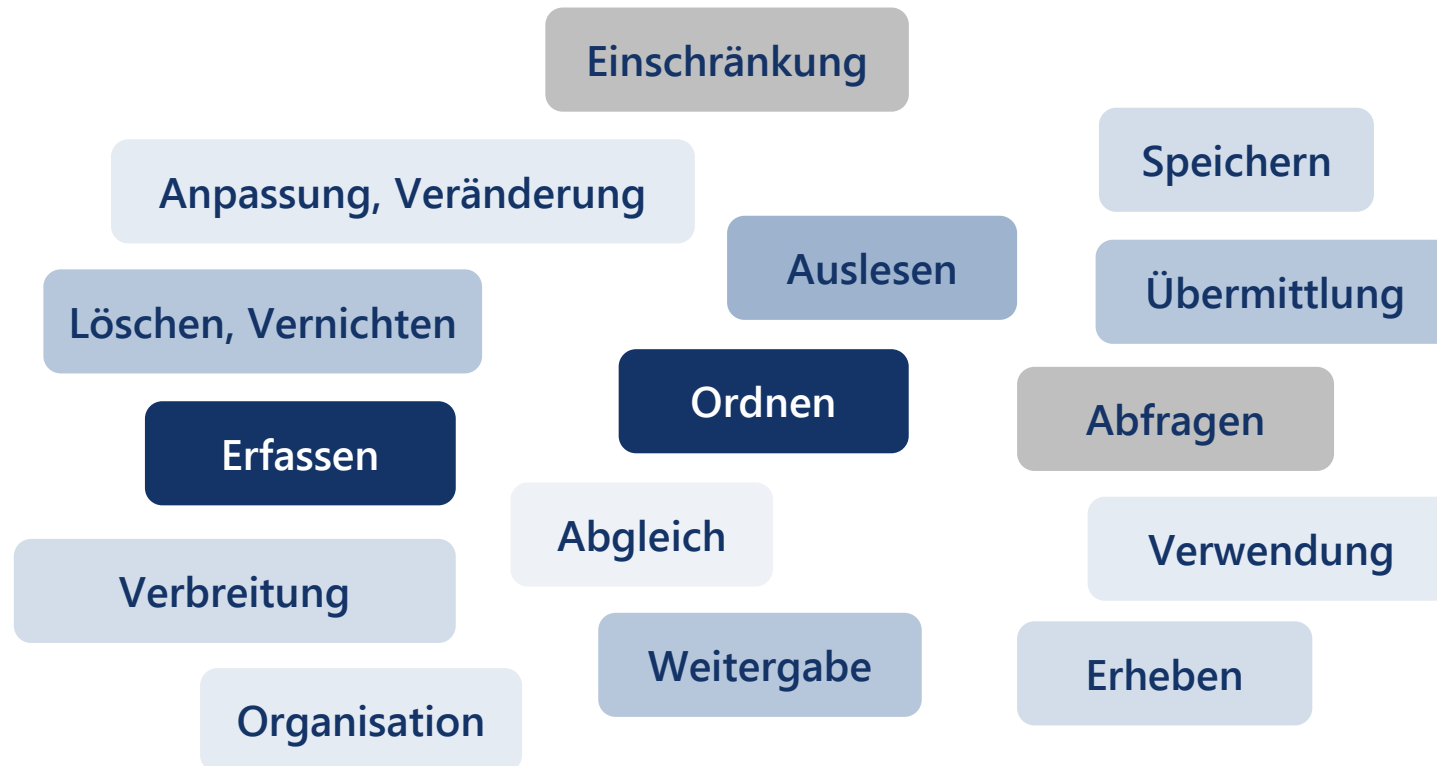
Alle Daten, aus denen die **rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen** oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten** oder **Daten zum Sexualleben oder der sexuellen Orientierung** einer natürlichen Person.

Die Verarbeitung solcher Daten ist grundsätzlich untersagt!

Ausnahmen:

- Ausdrückliche Einwilligung der betroffenen Person
- Verarbeitung erforderlich (Verpflichtung Arbeits- oder Sozialrecht; Schutz lebenswichtiger Interessen)
- Verarbeitung durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Einrichtung plus geeignete Garantien
- Daten von der betroffenen Person offensichtlich öffentlich gemacht
- ...

Verarbeitungen im Sinne der DSGVO



Rechtmäßigkeit der Verarbeitung

Art. 6 DSGVO

Eine Rechtsvorschrift erlaubt oder ordnet die Verarbeitung an.



Es liegt eine Einwilligung des Betroffenen vor.

Die Verarbeitung ist erforderlich, z.B.

- zur **Erfüllung eines Vertrags**,
- zur **Erfüllung einer rechtlichen Verpflichtung**,
- zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- **Rechenschaftspflicht**

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Rechenschaftspflicht (Accountability)

Art.5 Abs. 2 DS-GVO

„Der Verantwortliche ist für die Einhaltung des Art. 5 Abs. 1 DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht).“

Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO...

-
- | | |
|-----------------------------------|--------------------------------|
| Rechtmäßigkeit | Datenminimierung |
| Verarbeitung nach Treu und Glaube | Richtigkeit |
| Transparenz | Speicherbegrenzung |
| Zweckbindung | Integrität und Vertraulichkeit |
-

**Art. 5 DS-GVO - Grundsätze für die Verarbeitung personenbezogener Daten*

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Pflicht zur Bestellung eines DSB

Art. 37 DSGVO

Kerntätigkeit der Einrichtung ist die

- **umfangreiche regelmäßige und systematische Überwachung betroffener Personen** (z.B. Auskunfteien, Versicherungsunternehmen,...)

oder

- **umfangreiche Verarbeitung besonderer Kategorien von Daten oder von Daten über Straftaten** (z.B. Krankenhäuser, Labors, etc.)

Pflicht zur Bestellung eines DSB

Art. 37 DSGVO

- | Einrichtungen, bei denen **mind. 10 Personen in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind**

- | Einrichtungen, deren **Verarbeitung personenbezogener Daten einer Datenschutzfolgeabschätzung** unterliegt

- | Einrichtungen, die mit der **geschäftsmäßigen Verarbeitung personenbezogener Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung** befasst sind

Pflicht zur Bestellung

§ 36 KDG

Verpflichtend für folgende kirchliche Stellen

- die Diözese, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,

Für folgende kirchliche Stellen

- den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,
- die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform
- **nur** dann, wenn weitere besondere Voraussetzungen erfüllt sind (**10 Personen; Kerntätigkeit ist systematische Überwachung; Kerntätigkeit ist Verarbeitung besonders sensibler Daten**)

Pflicht zur Bestellung

§ 36 DSGVO-EKD

Verpflichtend für folgende evangelische Stellen, wenn:

bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind,

oder

die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.
Die Vertretung ist zu regeln.

Anforderungen an die Bestellung

Art. 37 DSGVO

Notwendige Qualifikation und persönliche Voraussetzungen

- Berufliche Qualifikation sowie Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie die Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben
- Verbot der Interessenkonflikte (kein GF, kein IT-Leiter, kein Vorsitzender...)

Form und Dauer der Bestellung

- Keine Vorgaben, Textform ratsam

Publizität der Bestellung

- Kontaktdaten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen

Möglichkeit der externen Bestellung sowie der Bestellung von Konzern-DSB`s

- Bestellung eines externen DSB`s sowie eines gemeinsamen DSB`s in Unternehmensgruppen möglich

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- **Stellung**
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Stellung des Datenschutzbeauftragten

Unabhängigkeit

- **Unabhängig** von fachlichen Weisungen
- Gewährleistung eines **unmittelbaren Berichtswegs** zur höchsten Managementebene

Abberufungsschutz und Benachteiligungsverbot

- Keine Abberufung bzw. Benachteiligung wegen der Erfüllung seiner Aufgaben
- Sonderkündigungsschutz nach § 6 Abs. 4 BDSG (Neu)
- Nach Abberufung noch ein Jahr Kündigungsschutz

Anspruch auf Einbindung, Unterstützung und Fortbildung

DSB als „Anwalt der Betroffenen“ / Pflicht zur Geheimhaltung bzw. Vertraulichkeit

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- **Aufgaben**

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Aufgaben des Datenschutzbeauftragten

Unterrichtung und Beratung

- Geschäftsführung
- Mitarbeiter

Überwachung der Einhaltung des Datenschutzes

- Kontrolle von Prozessen

Beratung bei der Durchführung der Datenschutzfolgeabschätzung

Zusammenarbeit mit der Aufsichtsbehörde

- Bearbeitung von Anfragen der Aufsichtsbehörde
- Meldung von Datenpannen

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- **Nachweis Erbringung/Dokumentation**
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Dokumentations- und Nachweispflichten

Grundsätze der Verarbeitung
- Art. 5 Abs. 2 DS-GVO,
Verantwortung des für die
Verarbeitung
Verantwortlichen - Art. 24
Abs.1 DS-GVO



Einwilligung - Art. 7 Abs. 1 DS-GVO,
Transparenz u. Modalität - Art. 12 ff.
DS-GVO,
Verzeichnis v. Verarbeitungstätigkeiten
- Art. 30 DS-GVO,
Benachrichtigung... - Art. 34 Abs. 2
DS-GVO,
DSFA - Art. 35 DS-GVO,
Auftragsverarbeiter - Art. 49 Abs. 6

Insbesondere für Auftragsverarbeiter

- | Verzeichnis der Verarbeitungen nach Art.30 Abs. 2
- | Dokumentation der Weisungen und der Weisungen für Drittlandstransfer

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- **Verzeichnis der Verarbeitungstätigkeiten**
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Verzeichnis aller Verarbeitungstätigkeiten und Führung

Das Führen des Verzeichnisses aller Verarbeitungstätigkeiten liegt in der Verantwortung des Verantwortlichen - nicht beim DSB - und ist verpflichtend!

- | „*Verzeichnis aller Verarbeitungstätigkeiten*“ (Art. 30 Abs. 2 DS-GVO)
 - **NEU:** alle durchgeführten Tätigkeiten der Verarbeitung (automatisiert und nicht-automatisiert)
 - Das Verzeichnis ist nicht öffentlich; **ABER:** Pflicht zum Zurverfügungstellen gegenüber der Aufsichtsbehörde besteht
 - Das Verzeichnis dient dem DSB zur Erfüllung seiner Aufgaben in Form von Beratung, als Information und der Überwachung der Gesetzmäßigkeit

Führen des Verzeichnisses aller Verarbeitungstätigkeiten

- | Der Verantwortliche kann den **DSB** mit der Führung des Verzeichnisses aller Verarbeitungstätigkeiten **beauftragen**
- | Das Verzeichnis dient dem DSB zur Erfüllung seiner Aufgaben in Form von Beratung, als Information und der Überwachung der Gesetzmäßigkeit
- | Darüber hinaus gibt das Verzeichnis dem Verantwortlichen und der Aufsichtsbehörde, auf Anfrage, einen Überblick über alle Verfahren die personenbezogene Daten verarbeiten
- | Zudem ist es ein effektives Mittel bezüglich der **Rechenschaftspflicht** und eine Voraussetzung für eine **Gesetzmäßigkeit**
- | Es unterstützt bei der Erstellung der Formulare zur Erfüllung der **Informationspflicht nach Art. 13**

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- **Transparenz- und Informationspflichten**
- Meldung von Datenpannen
- Datenschutzfolgeabschätzung

Erweiterte Transparenz- und Informationspflichten

Informationspflicht, wenn die Erhebung von Daten bei einer betroffenen Person sowie im Fall, wenn die Daten nicht bei der betroffenen Person erhoben werden

- | **Alle Informationen** müssen in präziser, klarer und leicht zu verstehender Sprache vorhanden sein
- | **Datenverarbeiter & Verarbeitungsrahmen:** bspw. Name und Kontaktdaten DSB und des Verantwortlichen, Rechtsgrundlage der Verarbeitung und Zweck, mögliche Empfänger, Dauer der Speicherung
- | **Weitergabe und Auslandsbezug**, Empfänger oder Kategorien der personenbezogenen Daten, Absicht der Übermitteln in ein Drittland, geeignete oder angemessene Garantien und die Möglichkeit, wie eine Kopie zu erhalten ist bzw. wo sie verfügbar ist

Erweiterte Transparenz- und Informationspflichten

- | **Betroffenenrechte** bspw. Recht auf Auskunft, Datenübertragbarkeit, Berichtigung, Löschung, Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung und ein Beschwerderecht bei Aufsichtsbehörde
- | **Mögliche Ausschlüsse**, wenn der betroffene Person die Informationen schon bekannt sind, bei unverhältnismäßigem Aufwand, bei Forschungszwecken zur Datenverarbeitung
- | **Bußgeldbewehrt** (*Art. 83 Abs. 5 lit. b*) sowie **Anspruch auf Schadenersatz** (*Art. 82 Abs. 1*)

Fazit erweiterte Transparenz- und Informationspflichten

- | **Feststellung der Fälle, in denen personenbezogene Daten erhoben werden**
- | **Erstellung eines Musterschreibens zur Information der Betroffenen mit den relevanten Angaben**
- | **Prüfung der versicherungsrechtlichen Situation:
*Sind Verstöße vom Versicherungsschutz umfasst?***

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- **Meldung von Datenpannen**
- Datenschutzfolgeabschätzung

Was ist eine Datenpanne?

Unter einer Datenpanne ist eine Verletzung des Schutzes personenbezogener Daten zu verstehen. Dies muss weder vorsätzlich noch fahrlässig geschehen.

- Im Zuge von Wartungsarbeiten ist bei der deutschen Post eine Datenbank mit 200.000 Adressen ungeschützt ins Internet geraten (quelle: www.zeit.de)
- Bei der Landesbank Berlin wurde eine Tasche mit Kundendaten (Kontodaten, Verdienstbescheinigungen, Kreditanträge) gestohlen (quelle: www.heise.de)

Aber auch:

- **Das Dienst-Notebook eines Mitarbeiters wird aus dem Auto gestohlen**
- **Ein Mitarbeiter verliert sein dienstliches Smart-Phone**

Meldepflicht bei Datenpannen

Art. 33 DS-GVO

Bei einer Datenpanne muss eine Meldung an die Aufsichtsbehörde erfolgen

(Art. 33 DS-GVO)

- | **Wann:** Binnen 72 Stunden ab Bekanntwerden der Datenpanne („ohne schuldhaftes Zögern“)
- | **Inhalt:** Name und Kontaktdaten des DSB, Anzahl der Datensätze, Beschreibung der Datenschutzverletzung und deren Folgen sowie welche Maßnahmen ergriffen wurden
- | **Ausnahme:** wenn kein Risiko für die Rechte und Freiheiten der Betroffenen Personen besteht
- | **Bußgeldbewehrt**
- | Der Betroffene muss vom Verantwortlichen **informiert** werden
- | Gleiches gilt für **Auftragsverarbeiter**

Themenplan

1. Überblick EU-DSGVO

- Aktueller Stand und Zeitplan
- Neuerungen und deren Konsequenzen
- Was sind personenbezogene Daten?
- Rechenschaftspflicht

2. Der Datenschutzbeauftragte nach der DSGVO

- Pflicht zur und Anforderungen an die Bestellung
- Stellung
- Aufgaben

3. Umsetzungshinweise

- Nachweis Erbringung/Dokumentation
- Verzeichnis der Verarbeitungstätigkeiten
- Transparenz- und Informationspflichten
- Meldung von Datenpannen
- **Datenschutzfolgeabschätzung**

Datenschutzfolgeabschätzung

Je nach Art, Umfang und Risiko einer Datenverarbeitung muss u.U. eine sogenannte Datenschutzfolgeabschätzung durch den Verantwortlichen durchgeführt werden.

Wann konkret muss eine Datenschutzfolgeabschätzung durchgeführt werden?

- i.d.R. bei Verwendung neuer Technologien (z.B. Einführung eines Dokumentenmanagement-Systems)
- Einsatz einer Videoüberwachung
- Einführung einer Zeiterfassung
- Schließsystem per RFID-Chip

Fazit gesteigerte Nachweis- und Dokumentationspflichten

- | **Die Dokumentationspflichten für datenschutzrelevante Vorgänge steigt**
- | **Einplanung des gesteigerten Aufwandes im Zuge der Umsetzung der DS-GVO**
- | **Die Verzeichnisse von Verarbeitungstätigkeiten müssen nach der DS-GVO angepasst werden**
- | **Prozesse müssen aufgebaut werden, um meldepflichtige Datenpannen bei Aufsichtsbehörden zu melden**
- | **Bei der Erstellung der Datenschutzfolgeabschätzung sind die neuen Verantwortlichkeiten zu beachten**

Vertragsmanagement

Überprüfung bereits geltender bzw. noch abzuschließender Verträge mit Datenschutzrelevanz dahingehend, ob die Anforderungen der DS-GVO eingehalten sind:

- Insb. Auftragsdatenverarbeitungsverträge
- Verträge über die Übermittlung personenbezogener Daten

Anpassung der „Alt“-Verträge

Fotografieren nach der DSGVO

Bisher Regelung über das Kunst- und Urheberrechtsgesetz §§ 22 + 23

- Recht am eigenen Bild

Aktuell: KUR nur noch geltend für journalistische, künstlerische, wissenschaftliche und literarische Zwecke

Jede Erstellung und Veröffentlichung braucht eine Rechtsgrundlage

- **Einwilligung (Art. 6 Abs. 1 lit. a)**
- **Vertrag (Art. 6 Abs. 1 lit. b)**
- **Eine Interessenabwägung (Art. 6 Abs. 1 lit. f)**

Fotografieren nach der DSGVO

| Interessenabwägung

- Vernünftige Erwartungen der betroffenen Person berücksichtigen
 - Können die betroffenen Personen zum Zeitpunkt der Erhebung der personenbezogenen Daten (also hier bei Anfertigung der Fotografie) und angesichts deren Umständen vernünftigerweise absehen, dass eine Verarbeitung zu bestimmten Zwecken erfolgen wird, z.B. zur Berichterstattung über eine Veranstaltung in einem Vereinsblatt, dürften den berechtigten Interessen des Verantwortlichen in der Regel der Vorrang einzuräumen sein.
 - Bsp.: Hochzeit, Schützenfest, Kindergartenfest, Meisterfeier

| Aber: heimliche, versteckt gemachte Fotos, Fotos, die Privat- oder Intimsphäre verletzen dürfen weiterhin nicht gemacht werden.

Fotografieren nach der DSGVO

Besondere Schutzbedürftigkeit der Betroffeneninteressen

- **Kinder sind besonders schutzbedürftig**
- **Veröffentlichung im Internet, Facebook**
- **Fotos von Situationen, die Rückschlüsse auf besondere Kategorien von Daten zulassen**

Konkret:

- **Bilder von Schützenfesten, Meisterfeiern, Kindergartenfesten usw. können zu INTERNEN Zwecken genutzt und veröffentlicht werden**
- **Für eine Veröffentlichung im Internet sollte immer eine Einwilligung vorliegen**

Sanktionen nach der DSGVO bzw.

BDSG (neu)

- | **Rechtslage bisher:** Bußgelder bis **300.000,00 EUR** pro Einzelfall
- | **Art. 83 DSGVO:** bis zu **20 Millionen Euro** oder bis zu **4% des gesamten weltweit erzielten Jahresumsatzes** im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist (Konzern-Umsatz).
- | **Bemessungskriterien in Art. 83 DSGVO** (z.B.: Art, Schwere und Dauer des Verstoßes; Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes; Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind; etwaige einschlägige frühere Verstöße; etc.)
- | **Anspruch auf Schadenersatz** (*Art. 82 Abs. 1*)
- | **Strafvorschriften § 42 BDSG (neu)**

Hinweise im Überblick

1. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
2. Verpflichten Sie alle Mitarbeiter auf das Datengeheimnis /Verschwiegenheit
3. Erheben, speichern und verarbeiten Sie personenbezogene Daten nur, wenn Sie eine Rechtsgrundlage hierfür haben.
4. Betroffene müssen über die Datenverarbeitungsvorgänge informiert werden.
5. Erheben, speichern und verarbeiten Sie nur die personenbezogenen Daten, die für den jeweiligen Zweck erforderlich sind und speichern Sie diese auch nur so lange, wie sie für die Erfüllung des Zwecks erforderlich sind.
6. Stellen Sie organisatorisch und technisch sicher, dass nur diejenigen Personen personenbezogene Daten einsehen und verarbeiten können, die dies auch rechtlich dürfen bzw. müssen.

Hinweise im Überblick

7. Betroffene haben verschiedene Betroffenenrechte wie z. B. das Auskunftsrecht oder das Recht auf Datenlöschung. Stellen Sie sicher, dass Sie diesen Rechten zeitnah nachkommen können.
8. Prüfen Sie, ob Sie einen Vertrag zur Auftragsverarbeitung benötigen.
9. Prüfen Sie, ob Sie eine Datenschutzfolgenabschätzung durchführen müssen. Diese ist immer dann durchzuführen, wenn ein hohes Risiko bei der Datenverarbeitung besteht.
10. Sind zehn oder mehr Personen mit der automatischen Verarbeitung personenbezogener Daten beschäftigt, muss ein Datenschutzbeauftragter benannt werden.
11. Dokumentieren Sie, wie Sie Daten verarbeiten und wie Sie Ihren Pflichten nachkommen.

Hinweise im Überblick

<https://www.datenschutzzentrum.de/dsgvo/> (kostenfrei herunterladen)

Praxis-Reihe: Datenschutzbestimmungen praktisch umsetzen

- **Datenschutz bei Vereinen**
- **Videoüberwachung**
- **Fotos und Webcams**
- ...

Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine

Herausgegeben vom Bayrischen Landesamt für Datenschutzaufsicht

ISBN 978-3-406-71662-1

Kosten: € 5,50

Haben Sie noch Fragen?

Vielen Dank für die Aufmerksamkeit!