IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Die Europäische Datenschutzgrundverordnung

EU-DSGVO

Ihr Referent: **Sascha Weller**

- Rechtsanwalt und externer Datenschutzbeauftragter (eDSB)
- Tätigkeit als eDSB seit 2009
- Geschäftsführender Gesellschafter des im Jahre 2010 gegründeten IDR – Institut für Datenschutzrecht (www.idr-datenschutz.de)

Dieser Vortrag ist **für Sie** da, deshalb:

- Sie können immer Fragen stellen.
- Wir haben ausreichend Zeit, Fragen zu diskutieren und zu erörtern.
- Sollten Ihnen nach dem Seminar noch Fragen einfallen, gibt es auch Lösungen!

Weshalb überhaupt die EU-DSGVO?

Weshalb überhaupt die EU-DSGVO?

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

- **das aktuell noch geltende BDSG trat erst 2009 in Kraft**
- **die EU war bestrebt, einheitliche Regelungen im Bereich des Datenschutzes zu treffen (Harmonisierung)**
- **am 14. April 2016 wurde die DSGVO vom Europäischen Parlament beschlossen und am 25. Mai 2016 im Amtsblatt veröffentlicht**
- **Übergangsfrist bis 25. Mai 2018**
- **Achtung: EU-Verordnungen geltend verbindlich und unmittelbar!**

- **aber: leider doch keine wirkliche Harmonisierung des Datenschutzes; Stichwort: Öffnungsklausel / BDSG neu**

  (bestes Beispiel: Anzahl der Mitarbeiter zur Bestellung eines DSB)

Weshalb überhaupt die EU-DSGVO?

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Die DSGVO erfindet den Datenschutz nicht neu:

Das Datenschutzniveau in Deutschland war bereits durch das BDSG alt sehr hoch. Die bekannten und vertrauten Grundsätze werden im Wesentlichen beibehalten und fortentwickelt, wie v.a.:

1. **Zweckbindung (s. nächste Seite)**
2. **Datenminimierung**
3. **Speicherbegrenzung (Identifizierung und Löschung, sofern Daten nicht mehr erforderlich sind)**
4. **Integrität und Vertraulichkeit (Gewährleistung einer angemessen Sicherheit durch technische und organisatorische Maßnahmen)**

Welche Grundregeln sind zu beachten?

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Die Zweckbindung

Schon bei der Erhebung der Daten muss der Zweck der Verarbeitung festgelegt sein.

Außerdem gilt:

- Es muss sichergestellt werden, dass der Verwendungszweck der erhobenen Daten nicht geändert wird.
- Die Daten sind sozusagen an den ursprünglichen Zweck gekoppelt.
- Deshalb ist es grundsätzlich verboten, Daten für einen anderen Zweck zu gebrauchen als den, der bei der Erhebung vorgesehen war.

Personenbezogene Daten - Begriffsklärung

- Die Grundlage des Datenschutzes ist das Grundrecht auf informationelle Selbstbestimmung (Art. 1 iVm Art. 2 GG).
- Da es um die informationelle Selbstbestimmung von Menschen geht, beschäftigt sich der Datenschutz nur mit **personenbezogenen Daten:**

  „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.“
- Vereinfacht gesagt:

  Angaben mit Hilfe derer man eine Person identifizieren kann.
- Die „Wichtigkeit“ oder die „Sensibilität“ der Daten spielt keine Rolle.

Beispiele:

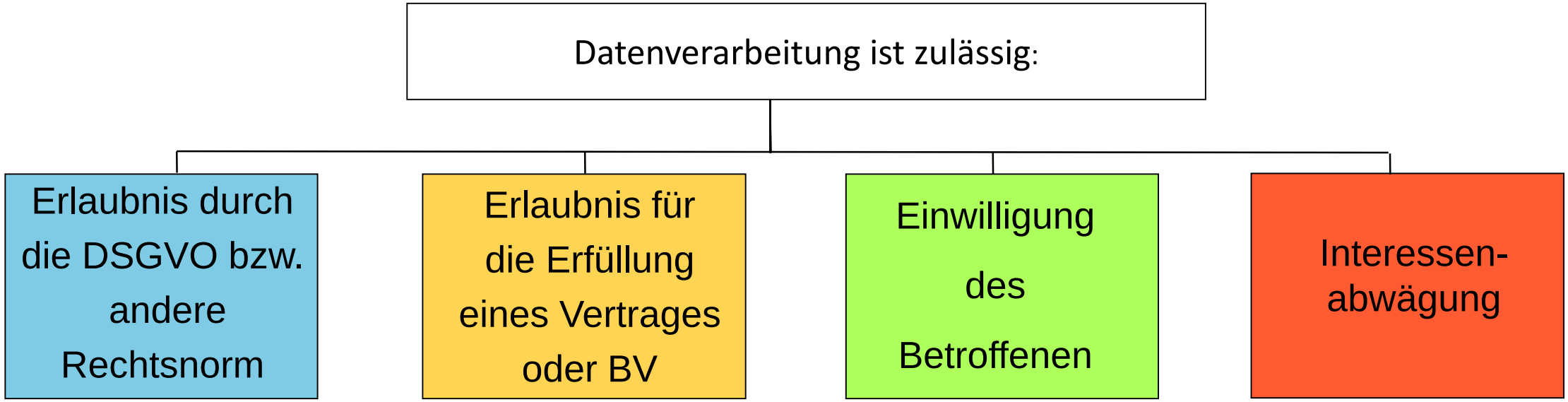
- **Vorname, Nachname**
- **Geburtsdatum**
- **Adresse**
- **Beruf**
- **Telefonnummer**
- **E - Mail - Adresse**
- **Gehalt**
- **Aussehen**
- **Geodaten**
- **Kontonummer**
- **IP – Adresse**
- **Kreditkartennummer**
- **…**

Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Welche Regeln sind für das Unternehmen besonders wichtig?

Wann dürfen Daten im Unternehmen verarbeitet werden?

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT



IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Erlaubnis für die Erfüllung eines Vertrages

Beispiele:

1. Daten aus dem Arbeitsvertrag, die die Durchführung des Arbeitsverhältnisses ermöglichen (Art. 88 DSGVO - Arbeitnehmer).

   Nicht: Bild des Mitarbeiters für die Unternehmenshomepage!

2. Daten aus anderen Verträgen, wie bspw. Kaufverträgen mit Kunden, die zur Durchführung dieser Verträge (und vorvertraglicher Maßnahmen) erforderlich sind.

   Nicht: Versand eines Newsletters an die Kunden!

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Einwilligung des Betroffenen

- Die Einwilligung des Betroffenen ist die logische Umsetzung der informationellen Selbstbestimmung.
- Um sicherzugehen, dass die Rechte des Betroffenen gewahrt bleiben, gibt es genaue Regelungen, die eine Einwilligung erfüllen muss.

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

- Die Einwilligung im Datenschutz muss **freiwillig** erfolgen.

  Kopplungsverbot!

- Die logische Konsequenz der Freiwilligkeit ist, dass der Betroffene seine Einwilligung jederzeit widerrufen können muss, ohne dass ihm dadurch Nachteile entstehen.

- § 4 a BDSG: Die Einwilligung muss grundsätzlich **schriftlich** erfolgen.

  DSGVO: **kein Schriftformerfordernis**; aber Nachweisbarkeit durch Unternehmen!

- Der Betroffene muss umfassend über die Datenerhebung und die geplante Verwendung informiert werden.

Rechte der Betroffenen

Welche Grundregeln sind zu beachten?

Rechte der Betroffenen

Alle von der Datenverarbeitung Betroffenen haben bestimmte Rechte. Die wichtigsten sind:

- **Das Recht auf Benachrichtigung/Information:**
  Grundsätzlich muss die verantwortliche Stelle dem Betroffenen mitteilen, dass sie Daten von ihm erhebt. Beispiele für Ausnahmen: Der Betroffene weiß dies bereits, oder die Erhebung der Daten ist von einem Gesetz ausdrücklich vorgeschrieben.

- **Auskunftsrecht:**
  Der Betroffene kann Auskunft verlangen. Es besteht eine Pflicht zur Auskunft (Art. 15 DSGVO), spätestens innerhalb eines Monats.

Welche Grundregeln sind zu beachten?

Rechte der Betroffenen

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

- **Berichtigung:**
  Falsche Daten sind zu berichtigen (Art. 16 DSGVO).

- **Löschung:**
  Personenbezogene Daten müssen gelöscht werden, z.B. wenn ihre Speicherung unzulässig ist (Art. 17 DSGVO).

  Beispiel: Löschung von Bewerberdaten nach drei Monaten!

Welche Grundregeln sind zu beachten?

Rechte der Betroffenen

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

- **NEU: „Recht auf Vergessenwerden“ (Art. 17 Abs. 2 DSGVO)**

  Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der folgenden **Gründe** zutrifft:

  - Die personenbezogenen Daten sind **für die Zwecke**, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht **mehr notwendig**.
  - Die betroffene Person **widerruft ihre Einwilligung**.
  - Die betroffene Person legt **Widerspruch gegen die Verarbeitung** ein.
  - Die personenbezogenen Daten wurden **unrechtmäßig verarbeitet**.

Welche Grundregeln sind zu beachten?

Rechte der Betroffenen

- **Datenübertragbarkeit (Art. 20 DSGVO)**

  Die DSGVO führt das Recht auf Datenübertragbarkeit ein, um der Anbieterabhängigkeit entgegenzuwirken. Eigentlich eine klare verbraucher- und wettbewerbsrechtliche Regelung!

Das Recht auf Datenübertragbarkeit bedeutet technisch:

- Bereitstellung von Daten in einem strukturierten, gängigen und maschinen-lesbaren Format (XML oder CSV) innerhalb eines Monats nach Kündigung.
- Prozess, um die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen zu übermitteln.
- Nach der Übertragung dürfen die Daten beim Übermittler nur noch zur Erfüllung gesetzlicher Aufbewahrungspflichten verwendet werden.

Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO

Verzeichnis von Verarbeitungstätigkeiten

Das Verfahrensverzeichnis des BDSG wird durch ein Verzeichnis aller Verarbeitungstätigkeiten abgelöst.

Unternehmen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis führen, es sei denn, der Verantwortliche verarbeitet personenbezogene Daten,

- die ein Risiko für die Rechte und Freiheiten der Betroffenen bergen (z.B. Scoring oder Überwachungsmaßnahmen) oder
- die besondere Datenkategorien oder Straftaten betreffen oder
- **nicht nur gelegentlich (z.B. regelmäßige Verarbeitung von Kunden- oder Mitarbeiterdaten).**

Verzeichnis von Verarbeitungstätigkeiten

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Die DSGVO sieht kein Einsichtsrecht für jedermann mehr vor!

Die Verzeichnisse müssen jedoch trotzdem erstellt und vorgehalten werden, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung gestellt werden müssen.

Inhalt:

Es müssen alle wesentlichen Angaben zur jeweiligen Verarbeitung beinhaltet sein, wie bspw. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten.

Zudem soll eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen enthalten sein (Art. 30 Abs. 1 lit. g und Abs. 2 lit d).

Beispiele:

- **Bewerberverfahren**
- **Personalakte**
- **Finanzbuchhaltung**
- **E-Mail**
- **Telefondatenbanken**
- **Webtracking**
- **uvm…**

Datenschutz auf der Unternehmenshomepage

Datenschutz auf der Unternehmenshomepage

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Auf der Homepage des Unternehmens sind insbesondere folgende Maßnahmen durchzuführen:

- Überarbeitung und Anpassung der Datenschutzerklärung
- Prüfung des Einsatzes von Trackingtools (Google Analytics, Matomo, etc.) und ggf. Integration in die Datenschutzerklärung
- Umstellung auf http**s://**
- Mitteilung des Datenschutzbeauftragten inkl. dessen Kontaktdaten (beachte: keine info@... E-Mail-Adresse)

zusätzlich: Meldung des DSB bei der zuständigen Aufsichtsbehörde

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Datenschutzbeauftragten bestellen!?

Mehr als 10 Personen (auch Selbstständige, Freiberufler, etc.), die ständig mit der Datenverarbeitung beschäftigt* sind oder Verpflichtung zur Datenschutz-Folgenabschätzung (z.B. wg. Videoüberwachung)?

Ja → **Pflicht zur Bestellung eines DSB**

Nein → **Werden biometrische Daten oder Gesundheitsdaten als Kerntätigkeit* umfangreich* verarbeitet?**

Ja → **Pflicht zur Bestellung eines DSB**

Nein → **Keine gesetzliche Pflicht zur Bestellung eines DSB**

* Noch keine/wenig Rechtsprechung zu diesen unbestimmten Rechtsbegriffen; deswegen im Zweifel, um keine Pflichtverletzung zu begehen, die Empfehlung, einen DSB zu bestellen.

Auftragsdatenverarbeitung

Haben Sie externe Unternehmen zur Erledigung Ihrer Arbeiten (Auftragsdatenverarbeiter) eingebunden?

Wenn „Ja“: Unbedingt eine **Übersicht der Auftragsdatenverarbeiter** erstellen und mit jedem Unternehmen einen **„Vertrag zur Auftragsdatenverarbeitung“** abschließen!

Beispiel:

1. Auslagerung der **E-Mail-Verwaltung** oder sonstiger Datendienste zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen)

2. **Auslagerung** der Back-Up-Sicherheitsspeicherung und anderer Archivierungen

3. **Datenträgerentsorgung** durch Dienstleister

4. **Prüfung oder Wartung durch IT- Dienstleister** (z. B. Fernwartung, externer Support), wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Folgen einer Datenpanne

Welche Regeln sind für das Unternehmen besonders wichtig?

Was passiert bei Datenpannen?

Es besteht – wie bisher - eine besondere Meldepflicht bei Datenpannen.

NEU: Datenpannen müssen künftig unverzüglich, **spätestens innerhalb von 72 Stunden** nach Bekanntwerden des Vorfalls an die zuständige Aufsichtsbehörde gemeldet werden.

Welche Regeln sind für das Unternehmen besonders wichtig?

IDR - WELLER
INSTITUT FÜR DATENSCHUTZRECHT

Was passiert bei Datenpannen?

Folgen für	das Unternehmen	die Geschäftsführung	den/die betroffenen Mitarbeiter
	Bußgeld bis 20 Mio. € / 4 % des Konzernumsatzes	Allgemeine zivilrechtliche Haftungsregeln (D&O – Versicherung)	Arbeitsrechtliche Konsequenzen: Ermahnung, Abmahnung, Kündigung, Haftung ggü. Arbeitgeber
	1. Schadensersatz-pflicht, Art. 82 DSGVO 2. Imageverlust	Ordnungswidrigkeit / Straftat: Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren	Ordnungswidrigkeit / Straftat: Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren

Special: WhatsApp

- WhatsApp lässt sich weit über 30 Berechtigungen geben.
- Unter anderem werden die Kontaktdaten, tlw. auch die Kalenderdaten, bei jeder Nutzung des Messengers abgeglichen, und neu hinzugekommene Kontakte auf Server in die USA übermittelt.

Vielen Dank für Ihre Aufmerksamkeit!

Sascha Weller
Rechtsanwalt und externer Datenschutzbeauftragter
Ziegelbräustraße 7
85049 Ingolstadt

ra-weller@idr-datenschutz.de
Tel.: 0841 – 885 167 15
Fax: 0841 – 885 167 22

Ich stehe Ihnen jederzeit sehr gerne für Rückfragen zur Verfügung, persönlich oder per E-Mail!