Das neue Datenschutzrecht ab 25. Mai 2018 – Anpassungsbedarf für HR

Leipzig, 27. Februar 2018

Zuhause in Leipzig

lwb

Vorstellung

Katja Rengers

Datenschutzbeauftragte der LWB mbH

- Konzerndatenschutz
- Beschäftigtendatenschutz
- Erfahrung als
  - Externe Datenschutzbeauftragte
  - Rechtsanwältin | Medien-/IT-/Datenschutzrecht


Alles neu,
macht der Mai

Relevante Normen der DSGVO zum Datenschutzmanagement

- **Art. 5**: Legt die Grundsätze zur Verarbeitung personenbezogener Daten fest

  → Datenschutz-Dokumentation und Nachweisführung (Rechenschaftspflicht)

> (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

> (3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

- **Art. 13 ff.**: Gestärkte Betroffenenrechte und Transparenzanforderungen

  → umfangreiche Informationspflichten gegenüber Betroffenen

- **Art. 30**: Verantwortliche müssen ein Verzeichnis der Verarbeitungstätigkeiten führen
- **Art. 32**: Regelt die Umsetzung von technischen und organisatorischen Maßnahmen (TOMs)

  → Risikobasierter Ansatz nach Stand der Technik

Was bleibt? - Datenverarbeitung nur mit Rechtsgrundlage oder Einwilligung

- Zur Datenerhebung/-verarbeitung von personenbezogenen Daten ist das Einverständnis des/der Betroffenen oder eine gesetzliche Grundlage nötig
- Nicht erforderliche Daten dürfen nicht erhoben werden
- Regellöschfristen müssen definiert werden | keine Datenspeicherung auf Vorrat
    - Löschung nach Zweckerreichung/Wegfall Erforderlichkeit
- Nur eine zweckbezogene Datenverarbeitung
- Berechtigungskonzepte bzgl. Zugriff auf Daten

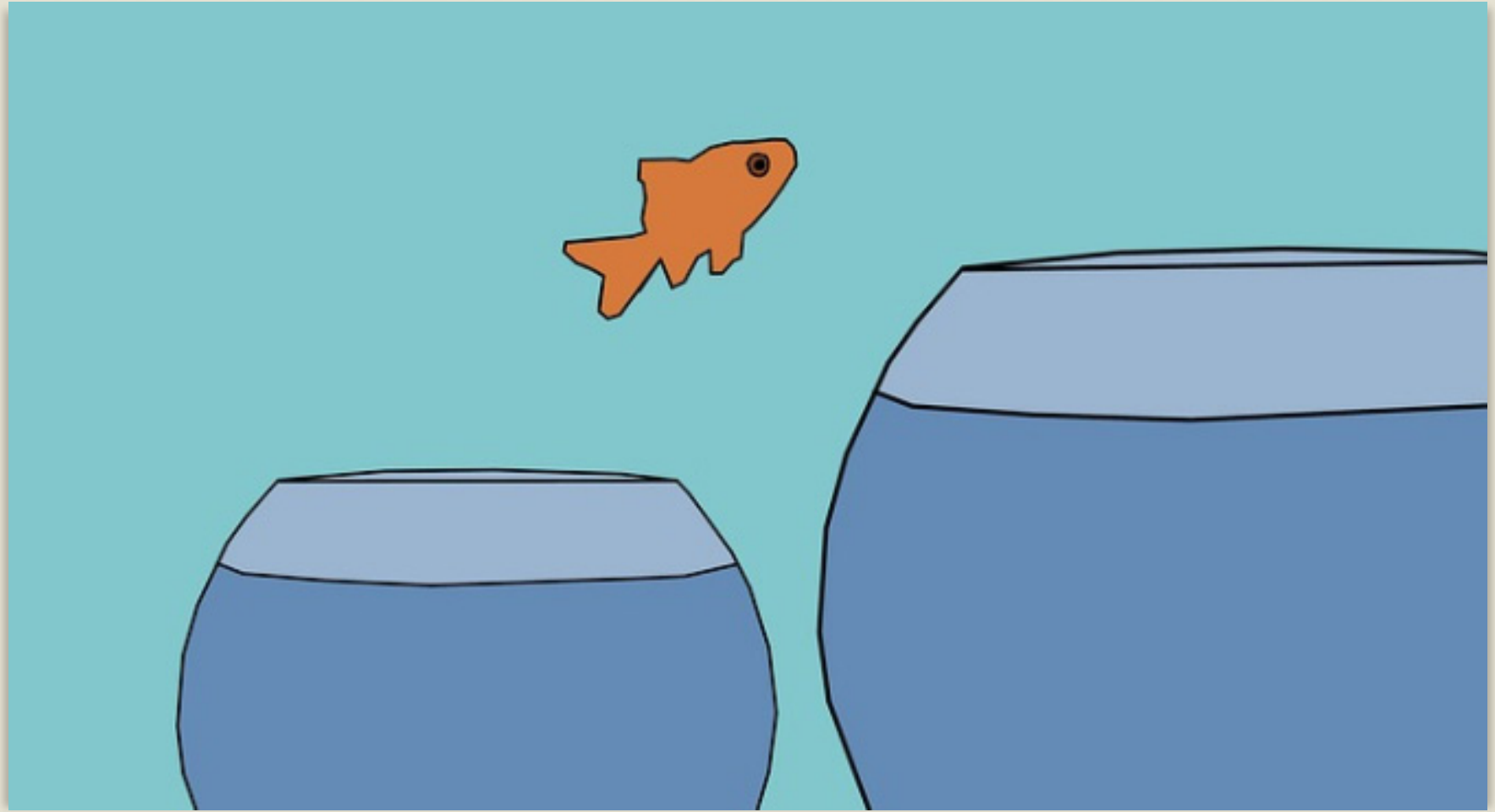
Verschärfung des Sanktionsrahmens bei Verstößen

> *Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*
>
> *a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43*

> *Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*
>
> *a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*

Wo liegt der Anpassungsbedarf?

- Dokumentation von Verarbeitungstätigkeiten
- Dokumentation von technischen und organisatorischen Maßnahmen
- Dienstleistermanagement: Auftragsverarbeitung/Vertragsverwaltung
- Prozess zur Wahrung der Betroffenenrechte
- Prozess zur Meldung von Sicherheitsvorfällen



Dokumentation von Verarbeitungstätigkeiten

- Bestandsaufnahme, wo personenbezogene Daten verarbeitet werden
- Sinnvolle Bündelung einzelner Prozesse zu einer Verarbeitungstätigkeit (Verfahren)
- Prozess zur zentralen Meldung neuer Verfahren/Prozesse (an DSB) entwickeln
- Typische Verarbeitungsübersichten:
  - (elektronische) Personaldatenverwaltung
  - Bewerbermanagement
  - Weiterbildung & Personalentwicklung
  - Arbeitszeiterfassung
  - Lohnabrechnung

Dokumentation von Verarbeitungstätigkeiten

Beschreibung der Verarbeitungstätigkeiten für Verantwortliche	
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Abteilung Name des Verantwortlichen Telefon E-Mail-Adresse	Personalabteilung
Bezeichnung der Verarbeitung, der Anwendung, des Programms	Bewerberverfahren
Zweckbestimmung der Verarbeitung	Auswahl geeigneter Bewerber zur Einstellung
Datenschutz-Folgenabschätzung mit Risikoanalyse ggf. Beschreibung in gesonderter Dokumentation	durchgeführt: ☐ ja am: ☒ nein, da nicht erforderlich Information an die Aufsichtsbehörde: ☐ ja am: ☐ nein, da nicht erforderlich Bemerkung:

Beschreibung der Kategorien betroffener Personengruppen	☐ Beschäftigte ☒ Interessenten ☐ Lieferanten ☐ Kunden ☐ Beschäftigte von Kunden oder Lieferanten ☐ Sonstige:
Beschreibung der diesbezüglichen Daten oder Datenkategorien	☐ Beschäftigtendaten ☒ Interessentendaten ☐ Lieferantendaten ☐ Kundendaten ☐ Beschäftigtendaten von Kunden oder Lieferanten ☒ Sonstige: Bewerbungsunterlagen, Anschrift Lebenslauf, Zeugnisse, Angaben zum beruflichen Werdegang Führungszeugnis Gesundheitszeugnis

Beschreibung der Verarbeitungstätigkeiten für Verantwortliche	
Empfänger oder Kategorien von Empfängern, denen die Daten offen gelegt sind oder werden	☒ intern Abteilung / Person Personalabteilung personalanfordernde Abteilung Geschäftsleitung betriebliche Mitarbeitervertretung

Dienstleistermanagement | Umgang mit externen Dienstleistern

- Gewissenhafte Auswahl von Dienstleistern: Zuverlässigkeit und Maßnahmen zu Datenschutz und Datensicherheit bereits vorab erfragen/prüfen
    - z.B. bei Einsatz von Software für Talent Pool, Personalverwaltung
- Frühzeitige Einbindung Datenschutzbeauftragter
- Nachweis ausreichender Schutzmaßnahmen
    - (interne Sicherheitskonzepte, Zertifizierungen,…)

- Vertragliche Vereinbarung zu Verpflichtung auf verantwortungsvollen Umgang mit Daten

  → Auftragsverarbeitungsverträge
- Verpflichtungen zur Geheimhaltung bei z.B. unabhängiger Beratern

Unterrichtung & Verpflichtung zur Geheimhaltung

- Dokumentierte Verpflichtung auf „Datengeheimnis“ = Maßnahme zur Erfüllung der Rechenschaftspflicht des Unternehmens
- *Wer?*

  – Regulärer Mitarbeiterstamm + Azubis + Praktikanten + Leiharbeiter + Freelancer
- *Wann?*

  – bei Aufnahme der Tätigkeit; regelmäßige Sensibilisierungen; Erneuerung bei Arbeitsplatz-/Aufgabenwechsel
- *Wie?*

  – Belehrung über die sich aus DSGVO/BDSG ergebenden Pflichten

Unterrichtung & Verpflichtung zur Geheimhaltung

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen[1]:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor un-

Betroffenenrechte für Beschäftigte

- Recht auf Auskunft, Berichtigung und Löschung der über sie gespeicherten Daten
- Recht auf Datenportabilität:

  = Recht, eine maschinenlesbare Kopie seiner Daten in einem gängigen Format zu verlangen, es sei denn, die Portierung der Daten beeinträchtigt die Rechte anderer Personen
- Darauf sollten Sie achten:
  - zeitnahes Reagieren auf Auskunftsanfragen
  - immer in Rücksprache mit Datenschutzbeauftragten
  - immer auf schriftliches Gesuch verweisen
  - nur soviel wie tatsächlich nötig beauskunften

Datenschutzhinweise zur Datenverarbeitung

- Informationspflicht nach Art. 13 DSGVO

1st level	2nd level
Namen und Kontaktdaten des Verantwortlichen	Namen und Kontaktdaten des Vertreters in der EU
	Kontaktdaten des Datenschutzbeauftragten
Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen	Rechtsgrundlage für die Verarbeitung
Berechtigte Interessen, die von einem Dritten verfolgt werden	Berechtigte Interessen, die von dem Verantwortlichen verfolgt werden

Kategorien von Empfängern	Empfänger
Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln	Vorhandensein oder das Fehlen eines Angemessenheitsbschlusses der Kommission oder einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist.
	Dauer der Speicherung oder Kriterien zur Festlegung dieser Dauer

	Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit
Verpflichtung, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte	Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich

- Als Anlage zum Arbeitsvertrag, in betrieblichem Intranet, in Betriebsvereinbarungen,…

Weitere Themen im Blick behalten

- Einwilligung im Arbeitsverhältnis ggf. erneuern/überprüfen (z.B. Fotogenehmigungen, Privatnutzung von E-Mail/Internet, beim betrieblichen Gesundheitsmanagement)
- ggf. Anpassung von Betriebsvereinbarungen um DSGVO-konform zu sein
- Kontrolle/Einführung von Datenlöschungen und Festlegung von Aufbewahrungsfristen
- Neben elektronischer Datenhaltung auch papierbasierte Datenhaltung überprüfen

Einige Quellen

- Zu Verarbeitungsübersichten: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
- Zu Verpflichtungserklärung: https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf
- Zu Transparenz- und Informationspflicht: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf
- Weitere Praxishilfen zur DSGVO:
  - https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
  - https://www.lda.bayern.de/de/datenschutz_eu.html

Vielen Dank

Katja Rengers
Datenschutzbeauftragte der LWB mbH

Telefon 0341 9924 9500
katja.rengers@lwb.de

Leipziger Wohnungs-
und Baugesellschaft mbH
Wintergartenstraße 4
04103 Leipzig

Zuhause in Leipzig