adreko
Die Alarmanlage für Ihre Daten

DS-GVO: Umsetzungs-Tipps für KMUs

Industrie- und Handelskammer zu Köln

Köln, 21.03.2018

Ihr Referent heute

Dirk Niedernhöfer

- Datenschutzbeauftragter (TÜV zert.) – seit 2010

  externer **DSB** in KMUs

- Geschäftsführer adreko GmbH – seit 2003

  Aufklärung von Datenmissbrauch und

  Kundendatendiebstählen

- Redakteur für Datenschutzthemen

- **datenschutzpraktiker.de**

  mit RA Rolf Becker von Wienke & Becker, Köln

Vorab: keine Rechtsberatung!

Ich plaudere aus der Praxis…

Vorab: 2 Quellen + 2 Buchtipps, die heute öfters auftauchen

Gesellschaft für Datenschutz und Datensicherheit e.V. – GDD

- gdd.de

Bayerisches Landesamt für Datenschutzaufsicht – LDA Bayern

- lda.bayern.de

Thomas Müthlein (Hrsg.): „Datenschutz-Grundverordnung General Data Protection Regulation: zweisprachige Textausgabe Englisch – Deutsch“

- ISBN-10: 3895777951 / Verlag Datakontext

Bayerisches Landesamt für Datenschutzaufsicht (Hrsg.): „Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket“

- ISBN-10: 3406716628 / Verlag C.H. Beck

Stichtag: 25.05.2018

- **Keine** Übergangsfrist!
- Umstellung auf **DS-GVO** kann bereits jetzt erfolgen.
  - BDSG gilt streng genommen bis zum 24.05.
- Wenn Sie noch nicht begonnen haben, starten Sie **jetzt**.

Personenbezogene Daten: wie BDSG

DS-GVO: „Personenbezogene Daten (pb-Daten) sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (…).“

Was sind personenbezogene Daten?

(Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen)

Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person sind:

- ***Name*, Alter,** *Familienstand,* **Geburtsdatum**
- ***Anschrift, Telefonnummer, E-Mail Adresse***
- *Konto-, Kreditkartennummer*
- *Kraftfahrzeugnummer, Kfz-Kennzeichen*
- *Personalausweisnummer, Sozialversicherungsnummer*
- *Krankendaten*
- ***Zeugnisse***

*Auch **Fotos**, Videoaufnahmen, Röntgenbilder oder **Tonaufnahmen** können personenbezogene Daten beinhalten.*

Für wen gilt die DS-GVO?

Für Unternehmen, Vereine, Spendenorganisationen, Arztpraxen… - unabhängig von ihrer **Größe**!

- Nur die **private** Datenverarbeitung ist ausgenommen.
- Wenn es überhaupt einmal Ausnahmeregelungen gibt, sind sie **schwammig** (Beispiel VVT).
- Bestellung zum Datenschutzbeauftragten (DSB) in Deutschland wie bisher unter **BDSG**.
  - Auch wenn kein DSB bestellt werden muss, gilt die DS-GVO!
  - DSB hat nichts mit dem Datenschutzbeauftragten des Bundeslandes zu tun (= Datenschutzaufsichtsbehörde).

Wer muss einen DSB „benennen“?

Deutschland nutzt eine s.g. Öffnungsklausel – maßgeblich sind Artikel 37, Abs. 1 DS-GVO **UND** §38 im neuen BDSG:

- Mindestens 10 Personen **ständig**…
  - Auch Teilzeit-, Zeitarbeiter oder Azubis zählen mit!

oder

- Verarbeitungen mit besonderem **Risiko** für die Betroffenen…

oder

- **geschäfts**mäßige Verarbeitung…

Wer muss einen DSB „benennen“?

Beispiel adreko – mit pb-Daten arbeiten **ständig**:

- 4 Vollzeit-Mitarbeiter
- 1 Azubi
- 2 Teilzeit-Mitarbeiter
- 1 Aushilfe

= werden 2 weitere Mitarbeiter eingestellt, die ständig mit pb-Daten arbeiten, wird adreko bestellpflichtig.

- Ich selbst kann als GF nicht DSB von adreko werden, da Interessenskonflikt.

Muss mein Unternehmen einen DSB benennen?

Praxistipp 1:

„Die Erste Hilfe zur Datenschutz-Grundverordnung“ enthält eine Checkliste zur Bestellpflicht eines Unternehmens (Ja/Nein).

Wer kann Datenschutzbeauftragter werden?

- **Interne** Lösung: Mitarbeiter des Unternehmens
  - Kündigungsschutz
  - „Berufliche Qualifikation“
  - „Fachwissen“
  - Vorsicht bei Interessenskonflikten!
  - Vielfältige Weiterbildungsangebote
  - Angemessene Ausstattung: Zeit / Budget / Mittel
- **Freiwillige** Benennung eines DSB möglich!
- **Externe** Lösung: Spezialist außerhalb des Unternehmens
  - Vertrag! / evtl. Bestell-Urkunde
  - Juristen / IT-Spezialisten / Sonstige
  - Aktuell schwierig, externe DSBs zu finden

DSB unter DS-GVO

Praxistipp 2:

GDD-Praxishilfe I informiert über den DSB unter der DS-GVO (gdd.de/downloads/praxishilfen).

Ihr Start: 6 Schritte zur Umsetzung der DS-GVO von der bayerischen Aufsichtsbehörde

1. Strukturen und Verantwortlichkeiten im Unternehmen schaffen.
2. Überblick über Verarbeitungen herstellen.
3. Auftragsverarbeiter prüfen.
4. Transparenz herstellen.
5. IT-Sicherheit und Datenschutz-Management dokumentieren.
6. Vorgehen im Fall von Datenschutzverstößen festlegen.

1.: Strukturen und Verantwortlichkeiten schaffen

- **Verantwortlich: der Geschäftsführer.**
- *Ist Ihr Unternehmen verpflichtet, einen DSB zu bestellen?*
- Benennen Sie einen Mitarbeiter als „Datenschutz-Koordinator“.
  - Vorsicht: berücksichtigen Sie den Zeitaufwand!
  - Informieren Sie zum Thema Datenschutz + machen Sie im Unternehmen klar, dass Datenschutz Priorität hat.

1.: Strukturen und Verantwortlichkeiten schaffen

Praxistipp 3:

GDD-Praxishilfe II beschreibt Verantwortlichkeiten und führt Sie in Richtung eines

- **Datenschutz-Management-Systems.**

1.: Strukturen und Verantwortlichkeiten schaffen

- Erstellen Sie eventuell abschließend ein Datenschutz-Organigramm.
  - Das Organigramm kann auch hilfreich sein, wenn Sie Prozesse zur Meldung an die Aufsichtsbehörden oder für den Umgang mit Anfragen von Betroffenen festlegen.

2. Überblick über die Verarbeitungen: was ist eine Verarbeitung?

„Als Verarbeitung wird (…) jeder (…) stattfindende Umgang mit personenbezogenen Daten (…) definiert“.

2. Überblick über die Verarbeitungen: wie mache ich das?

Artikel 30 DS-GVO: Jeder Verantwortliche führt ein **Verzeichnis aller Verarbeitungs-tätigkeiten** (= VVT), die seiner Zuständigkeit unterliegen. Starten Sie mit Ihren VVTs.

- Entscheidung für eine VVT-Vorlage:
  - GDD-Praxishilfe V: gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
  - „Erste Hilfe “ enthält ebenfalls ein VVT-Muster.
  - Beide Versionen haben ziemlich sicher „Rückendeckung“ der Aufsichtsbehörden.
  - (Weitere kostenlose VVT-Vorlagen vorhanden)

2. Überblick über die Verarbeitungen: was nehme ich in meine VVTs auf?

- Nicht zu „tief“ gehen – eher prozessorientiert auf die Verarbeitungen blicken. Beispiel: nicht jedes einzelne Word-Dokument ist eine eigene Verarbeitung – Ansatz Verarbeitung „Allgemeine Bürokommunikation“…
- Ca. 20 – 30 Verarbeitungen in einem durchschnittlichen KMU.
- Beispiele für typische Verarbeitungen (HR):
  - Lohnbuchhaltung
  - Zeiterfassung
  - Allgemeine Personalverwaltung
  - Bewerbungen
  - (…)

2. Überblick über die Verarbeitungen: VVTs

Das Führen der VVTs erzwingt einen guten Überblick über das Handling personen-bezogener Daten im Unternehmen. Anders gesagt: das VVT ist die **Basis** ihrer DS-GVO-Compliance.

- Nur die **Aufsichtsbehörde** erhält das VVT – auf Anfrage.
- VVTs müssen **aktuell** gehalten werden – achten Sie daher bei den aufgenommen Informationen auf deren Verfallsdatum und fügen Sie eine Versionsinformation ein.

2. Überblick über die Verarbeitungen: Beispiel VVT

Praxistipp 4:

GDD-Praxishilfe V stellt ein Muster zur Verfügung und gibt Ihnen Ausfüllhinweise:
gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

(Im Termin wurde das Muster gezeigt)

3. Auftragsverarbeitungen prüfen: was ist eine AV?

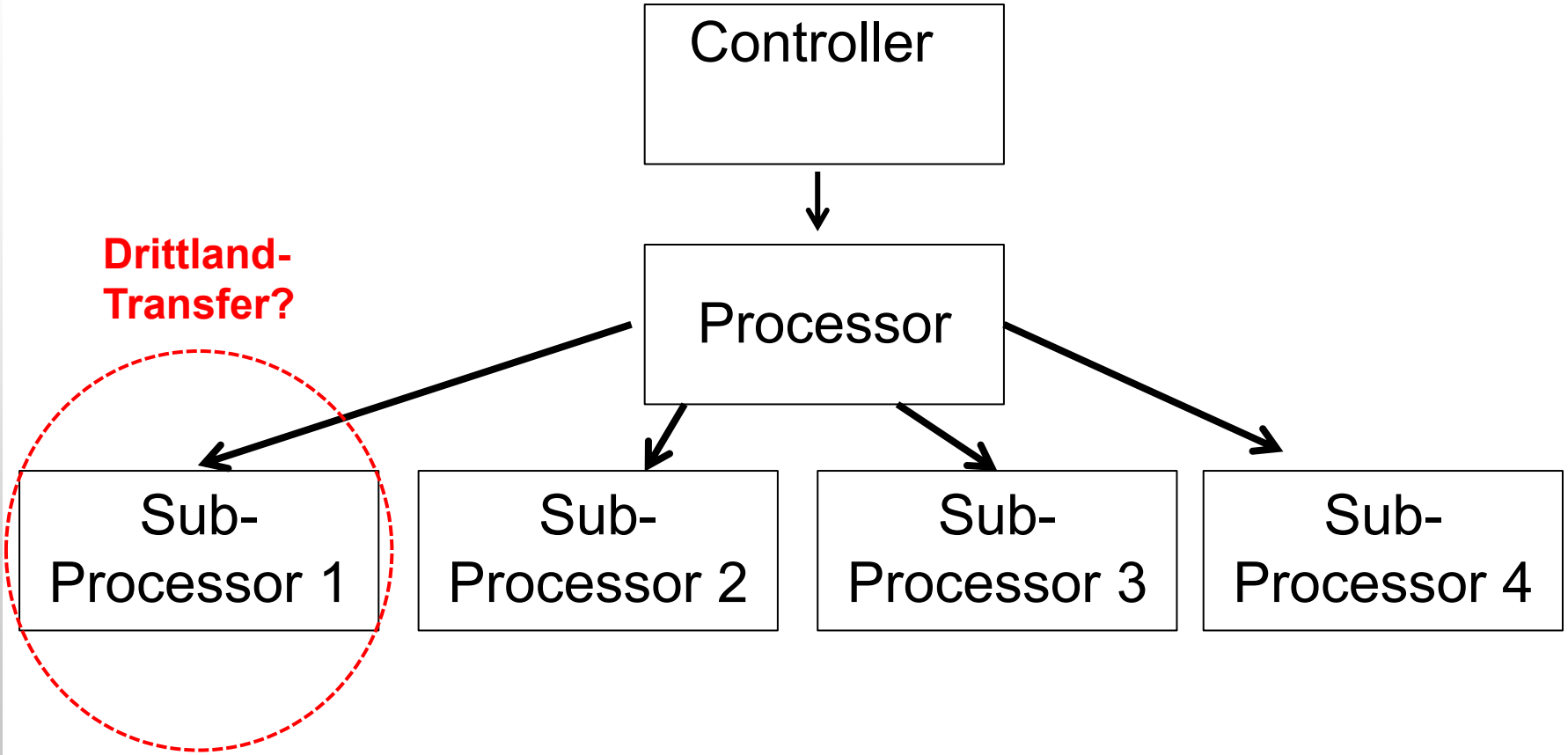
- „Geben“ Sie pb-Daten **außer Haus**? Wer entscheidet darüber, was mit diesen Daten passiert? Sie?
  - Nutzung von Cloud Services
  - Hosting der IT und/oder Webseiten
  - Externe Systemadministration (Streitfall!)
  - Externe Lohnbuchhaltung (DATEV!)
  - Zeiterfassungssystem
  - Drucker-Leasing
  - **Aktenvernichtung** oder –archivierung
  - (…)

- Die **Möglichkeit** eines Zugriffs reicht in der Regel aus.

3. Auftragsverarbeitungen prüfen: wie mache ich das?

- **Kein** Konzern-Privileg!
  - Gehen Daten zu einer Schwester-Firma **kann** auch das eine AV sein.
- **Dritt**staaten!
  - Außerhalb von EU und EWR liegt u.U. kein angemessenes Datenschutz-Niveau vor – dieses muss **vorab** sichergestellt werden.
  - Problem: USA, China, Japan…
  - (Ausnahme: die von der EU anerkannten sicheren Drittstaaten)
- **Vor-Ort-Kontrollen** kaum umsetzbar…

3. Auftragsverarbeitung



3. Auftragsverarbeitungen prüfen: wie mache ich das?

- Die Verarbeitung in Ihrem Auftrag muss **vertraglich** geregelt sein.
- Sie müssen sich von der **Eignung** des Dienstleisters überzeugen.
- Sie benötigen eine aktuelle **Übersicht** der laufenden Auftragsverarbeitungen.

3. Auftragsverarbeitungen prüfen

Praxistipp 5:

Vorlagen für Verträge zur Regelung einer Auftragsverarbeitung können Sie online bei der GDD (auch auf Englisch!) oder der bayerischen Aufsichtsbehörde abrufen.

4. Transparenz herstellen: was ist das?

Transparenzanforderungen nach Artikel 12 – 14 DS-GVO:

- Betroffene müssen umfangreich, **verständlich** und leicht abrufbar über die Verarbeitung ihrer Daten und ihre Rechte informiert werden.

4. Transparenz herstellen: was ist das?

An welchen Stellen werden bei Ihnen im Unternehmen pb-Daten erhoben?

- Website
- Telefon-Hotline
- Mailings + Kataloge
- Anzeigen + Beilagen
- Ladenlokale
- **Beschäftigte! / Bewerber!**

4. Transparenz herstellen: wie mache ich das?

- Website
  - Erweiterung der Datenschutzerklärung
- Telefon-Hotline
  - Abrufmöglichkeit / Versand per sms / mündlicher Verweis auf Webseite
- Mailings + Kataloge
  - Abdruck der „Minimalinformationen“ + Link auf Webseite
- Anzeigen + Beilagen
  - Abdruck der „Minimalinformationen“ + Link auf Webseite
- Ladenlokale
  - Aushang oder Handout
- **Beschäftigte! / Bewerber!**
  - Handout mit dem Arbeitsvertrag

4. Transparenz herstellen: darauf sollten Sie achten

- Übermittlung in Drittstaaten (angeben!)
- Löschfristen bzw. Speicherdauer

4. Transparenz herstellen

Praxistipp 6:

Der Deutsche Dialogmarketing Verband (DDV e.V. / ddv.de) gibt in seinem Best Practice Guide zur DS-GVO Formulierungsbeispiele zur Umsetzung der Transparenzanforderungen. Gute Lektüre für alle, die Direktmarketing betreiben!

- Online abrufbar unter ddv.de

5. IT-Sicherheit und Datenschutz-Management-System dokumentieren

IT-Sicherheit nach **Artikel 32 DS-GVO** – Sicherheit der Verarbeitung

- Berücksichtigung der Kosten!
- Risiko für die Betroffenen!

- Lassen Sie Ihren IT-Verantwortlichen sowohl die Dokumentation der IT aktualisieren als auch die aktuell getroffenen Sicherheitsmaßnahmen zusammenfassen.

5. IT-Sicherheit und Datenschutz-Management-System dokumentieren

Datenschutz-Management-System **nach Artikel 24 DS-GVO** – Verantwortung des für die Arbeit Verantwortlichen.

- Organisation – kein Tool
- Rechenschaftspflicht des Unternehmens!

5. IT-Sicherheit allgemein

Praxistipp 7:

Lassen Sie sich vom Begriff IT-Sicherheit nicht abschrecken! Sie können schon mit leicht umzusetzenden Maßnahmen viel erreichen.

- Vertraulichkeit
  - Umgang mit Daten in der Öffentlichkeit / Schulung der Mitarbeiter
  - Verschlüsselung von Daten auf mobilen Datenträgern
  - datenschutzgerechte Vernichtung ausgemusterter Datenträger
- Integrität
  - Berechtigungskonzepte
  - Zutrittsmöglichkeiten!
- Verfügbarkeit
  - BackUps

5. IT-Sicherheit – E-Mails

Praxistipp 8:

(Persönliche E-Mails sind pb-Daten.)

- Offene Kundenverteiler haben bereits in der Vergangenheit zu Bußgeldern geführt.
- E-Mail-Weiterleitungen im Unternehmen wurden von 1 Aufsichtsbehörde als unzulässig gewertet.
- **No Go**: pb-Daten als offener E-Mail-Anhang.
- In Fällen sensibler Daten sollte der E-Mail-Verkehr verschlüsselt erfolgen.

6. Vorgehen im Fall von Datenschutzverstößen

- Artikel 33, 1.: Verstöße sind vom Verantwortlichen möglichst innerhalb von 72 Stunden der **Datenschutz-Aufsichtsbehörde zu melden** – wenn ein Risiko für die Betroffenen besteht.

- Artikel 33, 2.: Wenn dem Auftragsverarbeiter eine **Verletzung des Schutzes personenbezogener Daten** bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

6. Vorgehen im Fall von Datenschutzverstößen: was ist das?

Mögliche Datenschutzverstöße - Beispiele:

- Externe Festplatte der Datensicherung wird bei einem Einbruch gestohlen.
- Eine Excel-Liste mit Namen und Gehältern von Mitarbeitern wird versehentlich an einen falschen E-Mail-Empfänger gesendet.
- Ein Vertriebsmitarbeiter verliert den Firmenlaptop mit der kompletten Kundendatenbank im Zug.

6. Vorgehen im Fall von Datenschutzverstößen: was ist zu tun?

Ein Datenschutzverstoß ist zu melden, wenn für die Betroffenen ein Risiko entsteht.

- Verpflichten Sie Mitarbeiter und Verarbeiter, Verstöße umgehend zu melden.
- Legen Sie fest, wer im Falle eines Falles im Unternehmen zu informieren ist.
  - GF + Justiziar + DSB + (…)
- Dokumentieren Sie jeden Verstoß! Halten Sie unbedingt fest, warum Sie entschieden haben, einen Verstoß nicht zu melden!

DS-GVO - wars das?

Nein.

- Recht auf Datenübertragbarkeit
- Zweckbindung
- 4-Wochen-Frist zur Bearbeitung von Anfragen Betroffener
- Löschung von Daten / Löschroutinen
- Data protection by design and by default
- Datenschutz-Folgeabschätzung
- (…)

Warnung – Rechtsunsicherheit!

- Vorsicht vor Erpressern!
- Bleiben Sie cool – nicht einfach zahlen.

3 Tipps zum Schluss

- Holen Sie sich morgen sofort die „Erste Hilfe“ (EUR 5,50 im Verlag C.H.Beck).
  - Denken Sie an Ihren Buchhändler um die Ecke.
- Bringen Sie Ihr Unternehmen anhand des enthaltenen Fragebogens auf Datenschutzkurs.
- Die Aufsichtsbehörden sind auch beratend tätig…

Kurze Zusammenfassung DS-GVO

Datenschutzverstöße werden ein echtes unternehmerisches Risiko – entsprechende Priorität ist dem Datenschutz auch im KMU einzuräumen.

- Es ist besser, noch nicht fertig zu sein, als nicht angefangen zu haben.

Danke.

adreko GmbH

Die Alarmanlage für Ihre Daten

Leostraße 84

50823 Köln

adreko.de

datenschutzpraktiker.de