Erste Erfahrungen DS-GVO

– Praxiserfahrungen aus Sicht der Aufsichtsbehörde –

Dr. Andrea Stubbe

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
(LDI) Nordrhein-Westfalen

IHK Köln, 22. Januar 2019

Übersicht

- Datenschutzaufsicht in Deutschland
- Herausforderungen für Unternehmen
- Informationspflichten, Art. 13/14 DS-GVO
- Auskunftsrecht, Art. 15 DS-GVO
- Meldepflichten, Art. 33/34 DS-GVO

Die Datenschutzaufsicht in Deutschland
Die Datenschutzkonferenz

https://www.datenschutzkonferenz-online.de/

Datenschutzaufsicht in Deutschland
Herausforderungen der Aufsichtsbehörden

- Wie hat sich das **Aufkommen** an Beschwerden und Auskunftsersuchen entwickelt?
- **Worauf** beziehen sich diese **Beschwerden** und sonstigen **Anfragen** vor allem?
- Welche Fälle von **Datenpannen oder Datenmissbrauch** wurden gemeldet?

Die Datenschutzaufsicht in Deutschland
Stichtag: 25. Mai 2018

- Zahlreiche Informationen auf den Webseiten:
  - Einstiegsinformationen
  - Kurzpapiere der DSK
  - FAQs etc…

- Schriftliche Beschwerden und Informationsanfragen mehr als verdoppelt in Jahr 2018 (ca. 11000)
- Ungezählte telefonische Anfragen

Datenschutzaufsicht
Ablauf bei Beschwerden

Je nachdem

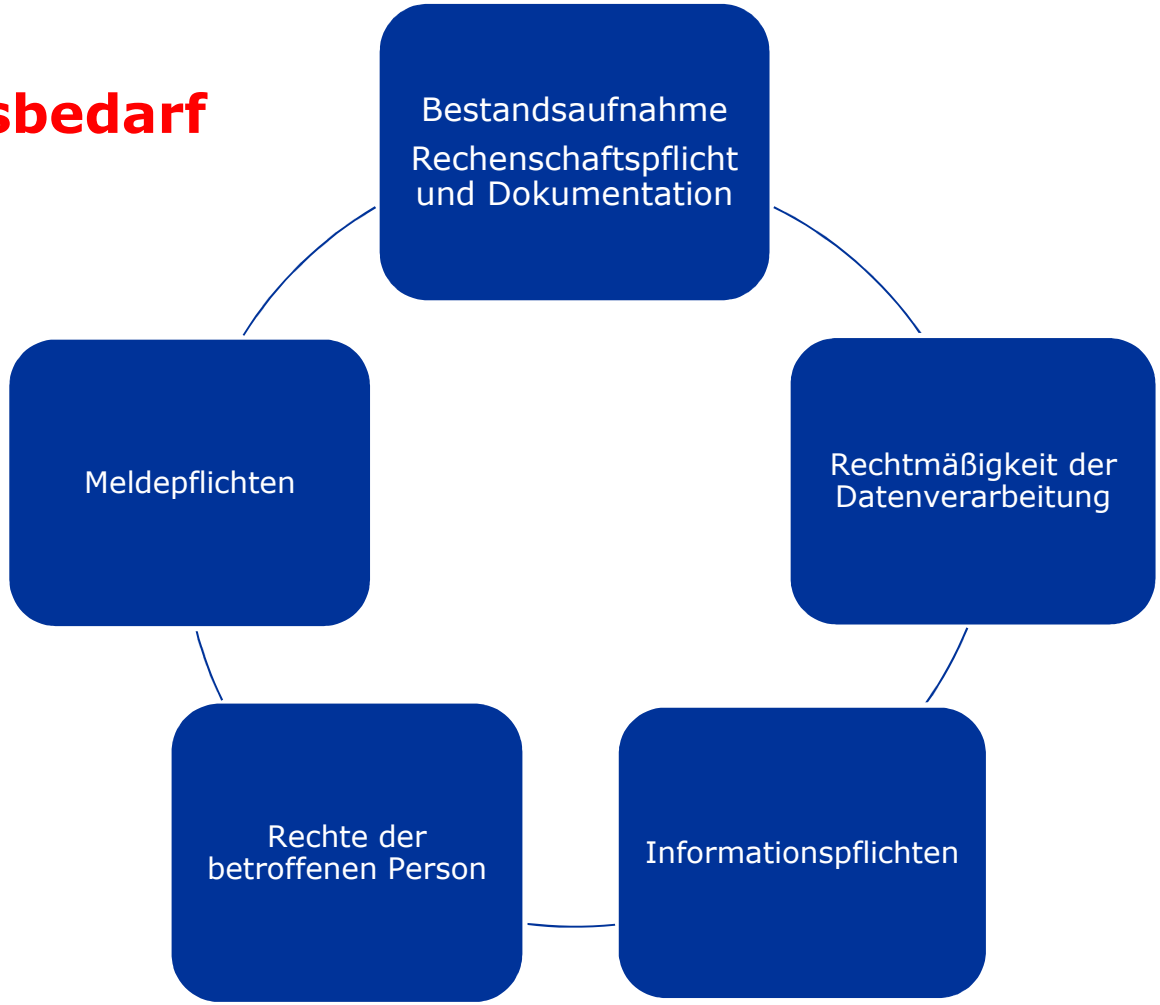
Geschäftsführer G von U

Herausforderungen für Unternehmen

Datenschutz ist Chefsache

Herausforderungen für Unternehmen

Änderungsbedarf klären !



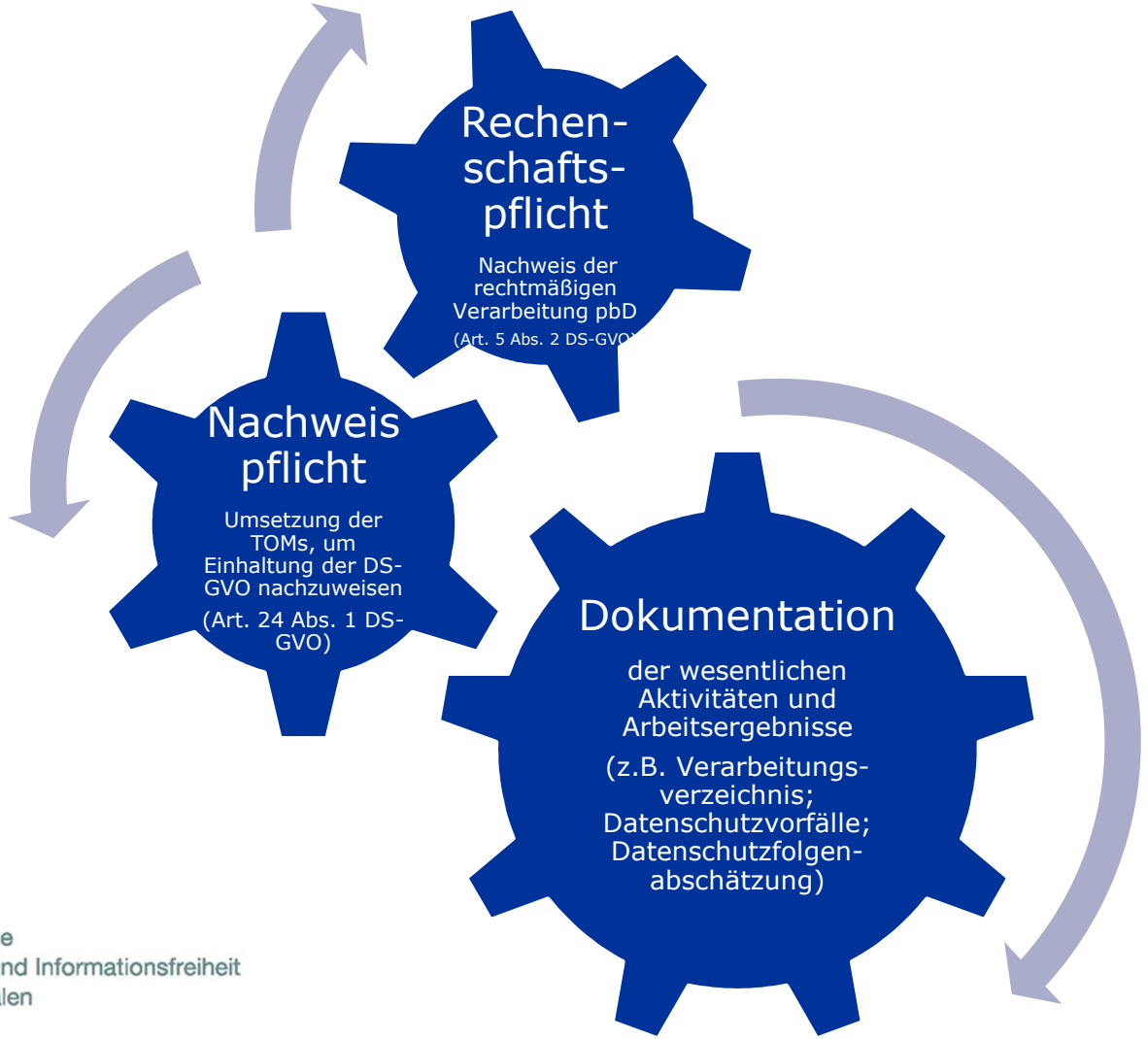
Hausforderungen für die Unternehmen

Bestandsaufnahme machen

- In welchen **Prozessen** im Unternehmen werden personenbezogene Daten verarbeitet?
- Gibt es **Produkte**, die das Unternehmen herstellt/vertreibt, die personenbezogene Daten verarbeiten? Falls ja, sind diese datenschutzfreundlich konzipiert bzw. voreingestellt?

Herausforderungen der Unternehmen

Rechenschaftspflicht/Dokumentation



Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 12: Einzelhändler – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Bekleidungshaus Huber
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: info@modehuber-fallstadt.de
Web: www.modehuber-fallstadt.de

Inhaber: Gerhard Huber, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über Buchhaltungsbüro)	Hans Klausen 0981/123456-1 hans@ modehuber-fallstadt.de	01.01.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer...	Buchhaltungs-büro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber-fallstadt.de	19.03.2018	Unternehmens-darstellung	• Kunden • Webseitenbesucher	• IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept
Kundenkarten-verwaltung	Marie Greiner 0981/123456-3 marie@ modehuber-fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	• Stammdaten der Kunden • Kaufhistorien	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber-fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	• Stammdaten der Kunden • Zahlungsdaten (Bank-verbindung)	Zahlungsdienst-leister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@ modehuber-fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	• Bestandskunden • potenzielle Neukunden	• Postadressen der Kunden	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Rechte der betroffenen Person

Transparenz als oberstes Gebot Art. 12 DS-GVO		
Information Art. 13, 14 DS-GVO	**Auskunft** Art. 15 DS-GVO	**Widerspruch** Art. 21 DS-GVO
	Berichtigung **Löschung** **Einschränkung** Art. 16 bis 19 DS-GVO	**Automatisierte Entscheidung** Art. 22 DS-GVO
	Datenüber-tragbarkeit Art. 20 DS-GVO	**Datenschutz-verstoß** Art. 34 DS-GVO

Vgl. auch **DSK-Kurzpapiere Nr. 6** (Auskunftsrecht), **Nr. 10** (Informationspflichten bei Dritt- und Direkterhebung) und **Nr. 11** (Recht auf Löschung)

Informationspflichten

- **Basis** für Ausübung der **Betroffenenrechte** (vgl. auch EG 60 – 62)
- **Art. 13 DS-GVO** für Direkterhebung / **Art. 14 DS-GVO** für Dritterhebung
- Informationspflichten gelten auch bei **Zweckänderung**!
- **Umfang:**
  - **Katalog** nach Art. 13 Abs. 1 und Abs. 2 DS-GVO, Art. 14 Abs. 1 und Abs. 2 DS-GVO
- **Pflicht zur Information besteht nicht** , wenn Person bereits über die Information verfügt (Art. 13 Abs. 4 und Art. 14 Abs. 5 lit. a DS-GVO);
  - weitere **Ausnahmen bei Dritterhebung**: z.B. Erteilung der Information ist unmöglich bzw. unverhältnismäßig oder zweckvereitelnd (Art. 14 Abs. 5 lit. b DS-GVO) oder Information unterliegt Geheimhaltungspflicht (Art. 14 Abs. 5 lit d DS-GVO); s.a. §§ 32 und 33 BDSG!
- **Form:** präzise, transparent, verständlich, leicht zugänglich, in klarer und einfacher Sprache (Art. 12 DS-GVO)
- **Frist**
  - bei Direkterhebung zum Zeitpunkt der Erhebung
  - bei Dritterhebung maximal Monatsfrist
- **Nachweis**
  - ordnungsgemäße Erledigung ist nachzuweisen (Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO)
- Vgl. auch **DSK-Kurzpapiere Nr. 10** (Informationspflichten bei Dritt- und Direkterhebung) und **DSK-Kurzpapier Nr. 3** (Verarbeitung personenbezogener Daten für Werbung)

Informationspflicht (Einzelfragen)

- **Gilt die umfangreiche Informationspflicht auch für Bestandskunden?**
  - **Ja**, wenn weitere personenbezogenen Daten des Betroffenen **erstmals erhoben** werden. Außerdem bei **Änderung des Verarbeitungszwecks**.

- **Ist ein Medienbruch bei der Informationsübermittlung zulässig?**
  - Ein Medienbruch, also ein Wechsel in der Kommunikationsform, ist nach Auffassung der LDI NRW unabhängig vom gewählten oder genutzten Kommunikationskanal **zulässig**.
  - Bei Direkterhebung sind **alle Informationen** nach Art. 13 Abs. 1 und Abs. 2 DS-GVO im **Zeitpunkt der Erhebung** der Daten **aktiv anzubieten**.
  - Die **wichtigsten Informationen** sind **auf dem Kommunikationsweg** mitzuteilen, in dem **zuerst** mit dem Betroffenen kommuniziert wird.

Informationspflicht (Einzelfragen)

- **Welche Informationen haben bei einem telefonischen Erstkontakt zu erfolgen?**
  - Ein **Verzicht** auf eine Datenschutzinformation ist **nicht möglich**. Der Verantwortliche muss nach Artikel 12 **geeignete Maßnahmen** ergreifen, um nach Artikel 13 bzw. Artikel 14 zu informieren.
  - Es sind z.B. folgende zulässige **Vorgehensweisen** denkbar:
    - Im Telefongespräch weist der Verantwortlichen **bei Beginn einer Datenverarbeitung** auf die **Verarbeitung** und ihren **Zweck** hin und bietet **aktiv** die weiteren Datenschutzinformationen an. Etwaige für die Betroffenen **überraschende Verarbeitungsschritte** (z. B. Drittstaatentransfer) müssen auch mitgeteilt werden. Auch teilt der Verantwortliche mit, **wo** die Informationen zu einem späteren Zeitpunkt **nachgelesen werden** können.
    - Es wird ein **telefonischer Ansagetext** mit den notwendigen Informationen eingespielt, der auf Knopfdruck abgespielt oder übersprungen werden kann. Die Wiederholbarkeit sollte dabei ebenso gewährleistet werden wie ein Hinweis, wo die Information bei Bedarf nachgelesen werden kann.
  - **Dokumentationspflichten** beachten!

Recht auf Auskunft

- **Umfang** (vgl. Katalog in Art. 15 Abs. 1 DS-GVO):
  - Verarbeitungszwecke
  - Kategorien personenbezogener Daten
  - Empfänger oder Kategorien von Empfängern, insbesondere in Drittländern
  - (falls möglich) Geplante Speicherdauer, ansonsten Kriterien für die Festlegung der Dauer
  - Bestehen eines Betroffenenrechts
  - Bestehen eines Beschwerderechts bei Aufsichtsbehörde
  - Wenn Daten bei einem Dritten erhoben werden: Herkunft der Daten
  - Wenn automatisierte Entscheidungsfindung: Aussagekräftige Informationen über die involvierte Logik, sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
  - Wenn Übermittlung an Drittländer: Unterrichtung über geeignete Garantien gemäß Art. 46 DS-GVO
- **Identitätsprüfung**
  - Es muss sichergestellt werden, dass die zu beauskunfteten Daten nicht unbefugten Dritten zur Verfügung gestellt werden.
  - Auswahl der Mittel für die Beauskunftung hat sich zwischen Datensparsamkeit und zielgerichteter Datenbeauskunftung zu bewegen.
- **Form**: schriftlich, elektronisch oder mündlich, möglichst in Form einer Datenkopie
- **Frist**: unverzüglich, spätestens innerhalb eines Monats zu erfolgen
- **Kosten**: Erste Datenkopie muss unentgeltlich erfolgen
- **Beschränkungsregelungen** (vgl. §§ 27 Abs. 2, 28 Abs. 2, 29 Abs. 1 S. 2, 34 BDSG-neu) schreiben bisherige Ausnahmeregelungen in § 19 und § 34 BDSG a.F. fort.
- **Vgl. auch DSK-Kurzpapier Nr. 6** (Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO)

Recht auf Auskunft (Einzelfragen)

- **Was ist eine Datenkopie im Sinne des Art. 15 Abs. 3 DS-GVO?**
  - Strittig! Tendenz zur restriktiven Handhabung: **Kein Herausgabeanspruch**, sondern „Abschrift", z. B. in Form einer **Übersicht** über die personenbezogenen (Inhalts-) Daten, also nicht komplette Akte.
- **Elektronische Beauskunftung (Art. 15 Abs. 3 S. 3 DS-GVO), aber wie?**
  - Noch nicht abschließend geklärt! Die **Identität** des Auskunftsersuchenden muss sichergestellt sein. Bei der elektronischen Zurverfügungstellung ist stets die **Datensicherheit** (Art. 32 DS-GVO) zu beachten, die von der **Sensibilität der Daten** abhängt.

Recht auf Auskunft (Einzelfragen)

Gibt es Grenzen des Auskunftsrechts?

- Liegen die genannten Voraussetzungen vor, kann die **Auskunft zunächst nur über die Stammdaten** mit der Bitte um Präzisierung zulässig sein.
  - *Vgl. Erwägungsgrund 63 a.E.: "Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt."*

- Beachtung der **Rechte und Freiheiten Dritter** (Art. 15 Abs. 4 DS-GVO)
  - **Güterabwägung** erforderlich, z.B. zwischen Auskunftsrecht und Recht des Verantwortlichen, seine Geschäftsgeheimnisse und Rechte des geistigen Eigentums wie Urheberrecht an Software zu schützen (Erwägungsgrund 63)
  - Als Ausnahme **restriktiv** zu handhaben!

- **(Häufige) Wiederholungen** von Auskunftsanträgen können zu Kostenerstattungspflicht (Art. 15 Abs. 3 S. 2 DS-GVO) oder Ablehnung (Art. 12 Abs. 5 S. 2 lit. b DS-GVO) führen.

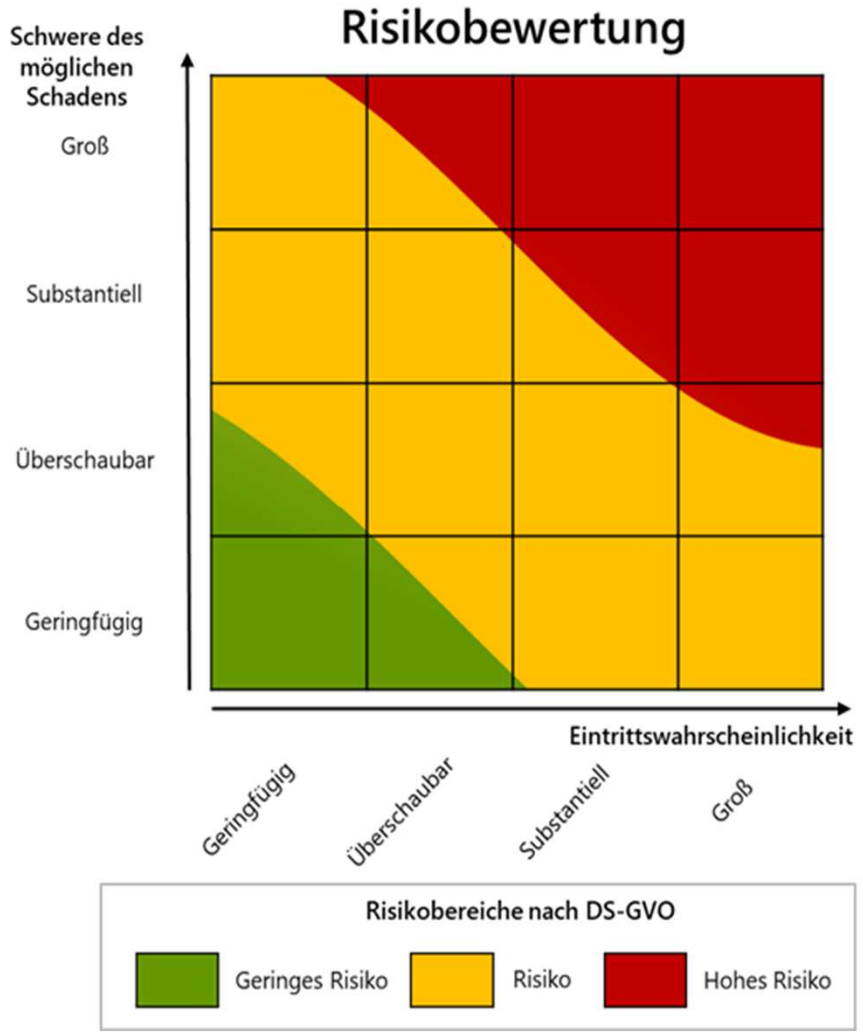
Meldepflichten nach der DS-GVO

Verletzung des Schutzes personenbezogener Daten

Meldung bei Verletzung des Schutzes personenbezogener Daten Art. 33 DS-GVO	Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Art. 34 DS-GVO
Verantwortlicher gegenüber **Aufsichtsbehörde** **aber:** Auftragsverarbeiter gegenüber Verantwortlichen	Verantwortlicher gegenüber **betroffener Person**
Frist: innerhalb von 72 Stunden nach Bekanntwerden	**Frist**: unverzüglich
Entfällt (nur dann), wenn **Risiko** für die Rechte und Freiheiten natürlicher Personen **ausgeschlossen** ist *oder Datenschutzverletzung nur **zu einem geringen Risiko** führt.*	Muss **nur erfolgen** • bei voraussichtlich **hohem Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen und kein Fall des Art. 34 Abs. 3 DS-GVO vorliegt oder • auf Verlangen der Aufsichtsbehörde
Im **Zweifelsfall**: Zuständige Aufsichtsbehörde kontaktieren **Vgl. auch DSK-Kurzpapier Nr. 18** (Risiko für die Rechte und Freiheiten natürlicher Personen)	

Risiko

- Risikobewertung
  - Schwere des möglichen Schadens
  - Eintrittswahrscheinlichkeit
- Risiko für die Rechte und Freiheiten (vgl. auch EG 85 DS-GVO)
- Blickwinkel der betroffenen Personen



Verletzung des Schutzes personenbezogener Daten (Einzelfragen)

- **Ist ein nur temporärer Verlust ausreichend?**
  - **Ja**, sofern dadurch die Gefahr unbefugter Zugriffe bestand.

- **Genügt es, wenn ein unbefugter Zugriff innerhalb der Stelle des Verantwortlichen stattfand?**
  - **Ja**, nach dem sog. Need-to-know-Prinzip genügt es, wenn ein unbefugter Zugriff innerhalb der Stelle des Verantwortlichen stattfand.

- **Löst der Verdacht eines unbeabsichtigten Verlusts oder eines unbefugten Zugriffs die Meldepflicht aus?**
  - Strittig! Maßgeblich ist, ob Verantwortlicher **hinreichend Informationen** hat, um beurteilen zu können, ob mit **hoher Wahrscheinlichkeit** eine Datenschutzverletzung eingetreten ist oder unmittelbar bevorsteht.

Verletzung des Schutzes personenbezogener Daten (Einzelfragen)

- **Ab wann gilt bei Datenpannen die 72 Std.-Frist zur Abgabe der Meldung?**
  - Die Meldung hat nach Art. 33 Abs. 1 **unverzüglich**, grundsätzlich innerhalb der 72 Stunden zu erfolgen. Die 72 Std.-Frist beginnt **mit dem Bekanntwerden**.

- **Sind Compliance-Fehler meldepflichtig?**
  - Compliance-Fehler **sind meldepflichtig**, sofern sie zu einer **Verletzung des Schutzes personenbezogener Daten** führen (Art. 4 Nr. 12 DS-GVO).

Weitere Hinweise für Unternehmen

- Was hilft bei der **Auslegung**?
  - **Erwägungsgründe** der DS-GVO (EG)
  - **Richtlinien/Guidelines** des Europäischen Datenschutzausschusses („Ausschuss"/„Board")
  - **Kurzpapiere** der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK) – abrufbar z.B. unter https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html
- Was hilft bei der **Anwendung**?
  - DSGVO-Text mit **Zuordnung** der Vorschriften des BDSG-neu und der Erwägungsgründe
    - vgl. z.B. GDD-Praxishilfe DS-GVO VI – abrufbar unter https://www.gdd.de/aktuelles/startseite/synopse-ds-gvo-und-neues-bdsg
  - **Anregungen für Unternehmen** - abrufbar z.B. unter https://www.ldi.nrw.de
    - "Maßnahmenplan DS-GVO" für Unternehmen, DSK-Kurzpapier Nr. 8
    - Fragenliste/Checkliste für kleine und mittlere Unternehmen
    - Neu: Umsetzungshilfe zu den Informationspflichten nach Art. 13, 14 DS-GVO

Weitere Hinweise für Unternehmen

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/index.html:

LDI NRW Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Auf dem Weg zur EU Datenschutz-Grundverordnung—Anregungen für Unternehmen
Die europäische Datenschutz-Grundverordnung (DS-GVO) bringt eine Reihe von Veränderungen in den datenschutzrechtlichen Anforderungen für den Umgang mit personenbezogenen Daten mit sich. Auch Auftrags(daten)verarbeiter müssen sich auf geänderte Rahmenbedingungen einstellen. Wir haben in 10 Punkten Anregungen für Unternehmen mit Sitz in NRW zusammengestellt.

1. Sensibilisierung durchführen

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.05.2018 nicht nur der Name einer europäischen Datenschutzregelung ändern wird. Die DS-GVO wird direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DS-GVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DS-GVO geben.

Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das Bundesdatenschutzgesetz!

2. Bestandsaufnahme machen

Um Änderungsbedarf identifizieren zu können, sollte in einem

5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design" und „Privacy-by-Default") umsetzen

Die DS-GVO enthält bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 DS-GVO).

6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftrags(daten)verarbeitung überprüfen und überarbeiten. In den Artikeln 26 bis 28 DS-GVO sind Vorgaben für Vereinbarungen mit Auftrags(daten)verarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

7. Datenschutzfolgeabschätzung implementieren

Weitere Fragen?

- Landesbeauftragte
  für Datenschutz und Informationsfreiheit
  Nordrhein-Westfalen

  Postfach 20 04 44
  40102 Düsseldorf

  Telefon: 0211 38 424-0
  Telefax: 0211 38 424-10

  www.ldi.nrw.de
  poststelle@ldi.nrw.de

Vielen Dank für Ihre

Aufmerksamkeit!