Tag der offenen Tür in Kiel und Neumünster, Update DSGVO

Tina Möller, Syndikusrechtsanwältin der IHK zu Kiel, 22.11. und 24.11.2023

EU-Datenschutzgrundverordnung

- **Merkblätter mit Vordrucken, Mustern etc. unter:**

  www.ihk-schleswig-holstein.de

  Dokumentennummer: 3971012

Must-haves:

- Nach außen **veröffentlichen**: Datenschutzinformationen (Informationspflichten) zentral auf der Homepage

- Nach innen **dokumentieren**: Verarbeitungsverzeichnis führen, Auftragsverarbeitungsverträge abheften, regelmäßige Schulungen der Mitarbeiter, Einwilligungen aufbewahren, Vorgänge zu Auskunftsansprüchen und Datenpannen ablegen, Bestellung des Datenschutzbeauftragten falls notwendig

Check-Liste

- Homepage aktuell halten, Informationspflichten!
- Verarbeitungsverzeichnis fortlaufend führen
- Technisch-organisatorische Maßnahmen einhalten
- Dokumentation der TOMs!
- Betroffenenrechte (Auskunftsansprüche!) beachten
- Meldepflichten bei Datenschutzverstößen einhalten
- Auftragsdatenverarbeitungsverträge ablegen
- Einwilligungserklärungen im Blick behalten
- Datenschutzbeauftragter bestellt?
- Beschäftigtendatenschutz sicherstellen

Datenschutzinformationen auf der Homepage

1. Name und Kontaktdaten des Verantwortlichen
2. Kontaktdaten des Datenschutzbeauftragten
3. Zweck und Rechtsgrundlage der Datenverarbeitung
4. Weitergabe/Empfänger der personenbezogenen Daten, Drittland?
5. Dauer der Speicherung der Daten
6. Hinweis auf das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung sowie auf ein Widerspruchsrecht
7. Hinweis auf Recht zum Widerruf einer gegebenen Einwilligung
8. Beschwerderecht bei der Aufsichtsbehörde
9. Hinweis auf Profiling etc.

Verarbeitungsverzeichnis pflegen

- Benennung der Verarbeitungstätigkeit
- Zweck der Verarbeitung
- Verantwortlicher bzw. Vertreter
- Datenschutzbeauftragter
- Aufsichtsbehörde
- Art der eingesetzten DV-Anlagen und Software, Programme
- Beschreibung der betroffenen Personen
- Benennung der Kategorien von Daten
- Empfänger der Daten (AVV´s)
- Drittlandübertragung
- Löschfristen
- TOM´s

Datenschutzbeauftragte

- förmliche schriftliche Bestellung notwendig, wenn sich im Betrieb mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen
- Wahl zwischen betrieblichem oder externem DSB
- der betriebliche DSB muss weisungsunabhängig sein
- Interessenkollision ausschließen (nicht IT-Leiter oder Personalleiter)
- Fachkunde und Zuverlässigkeit des DSB nachweisen
- Meldung des DSB an Aufsichtsbehörde (online möglich beim ULD)
- Publikation des DSB (z. B. auf der Webseite des Unternehmens)
- besonderer Kündigungsschutz für den betrieblichen DSB

Dokumentation!

Organisatorische Anforderungen an Unternehmen

- Anforderungen an wirksame Einwilligungserklärungen:

1. Information über Zweck und Umfang der verarbeiteten Daten
2. Erklärung muss leicht zugänglich in leicht verständlicher Form in klarer und einfacher Sprache verfasst sein
3. Hinweis auf jederzeitiges Widerrufsrecht
4. Beachtung des Kopplungsverbotes
5. Double opt in bei Newslettern
6. keine Einwilligung von Minderjährigen unter 16 Jahren möglich
7. kein Schriftformerfordernis mehr (auch elektronisch möglich)
8. Beweislast liegt beim Verantwortlichen

Beispiel Autohaus mit 30 Mitarbeitern

- Arbeitsabläufe mit Personendaten identifizieren/auflisten

– Kundenkontakte (Telefongespräche, Terminvergabe etc.)
– Mailingaktionen
– Kaufabwicklung
– Rechnungswesen
– Mitarbeiterverwaltung
– Reparaturbetrieb
– usw.

Beispiel Autohaus mit 30 Mitarbeitern

- Rechtsgrundlagen für Datenverarbeitung hinterfragen/notieren

– Vertragsanbahnung (berechtigtes Interesse)
– Mailingaktion (Einwilligung oder berechtigtes Interesse)
– Kaufabwicklung (Vertrag)
– Rechnungswesen (Vertrag)
– Reparaturservice (Vertrag)
– Mitarbeiterverwaltung (Vertrag)
– Aufbewahrung der Vertragsunterlagen für 10 Jahre (Gesetz)

Technische Anforderungen an Unternehmen

- Schutz vor unbefugtem Zutritt, Zugang und Zugriff
- Einsatz datenschutzfreundlicher Technologien
- Privacy by design and Privacy by default
- Stand der Technik als Anforderung an die IT-Sicherheit
- Verschlüsselung und Pseudonymisierung bei Datenübertragung
- Berechtigungskonzept (Trennungsgebot)
- Firewall, Virenschutz

Organisatorische Anforderungen an Unternehmen

- Dokumentationspflichten bei jeder Art von Datenpannen
- Meldepflicht gegenüber der Aufsichtsbehörde innerhalb von 72 Stunden, Ausnahme: Wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte der betroffenen Person führt.
- Mitteilungspflicht an die Betroffenen nur bei hohem Risiko für den Betroffenen, Ausnahme: Wenn durch Maßnahmen sichergestellt ist, dass das hohe Risiko beseitigt wurde oder die Information an Betroffene mit unverhältnismäßigem Aufwand verbunden wäre.

Die größten DSGVO-Irrtümer nach wie vor:

- Ich muss immer alle meine Kunden anschreiben und die Datenschutzinformationen mitschicken oder auf sie hinweisen.
- Ich brauche für jede Speicherung von Personendaten eine Einwilligung.
- Ich muss mir die Datenschutzerklärung bestätigen lassen.
- Ich brauche zu jedem Vertrag auch einen Auftragsverarbeitungsvertrag.
- Jede Datenweitergabe bedarf der Einwilligung der Betroffenen.
- Ich darf keine Fotos mehr machen ohne Einwilligung.

Mögliche Risiken

- anonyme Meldungen an die Aufsichtsbehörde durch Konkurrenten, unzufriedene Kunden oder ehemalige Mitarbeiter
- öffentlichkeitswirksame Datenlecks oder Hackangriffe
- anlasslose Prüfungen der Datenschutzaufsicht
- Abmahnung von Datenschutzverstößen durch Konkurrenten oder Vereinen
- Bußgelder durch Aufsichtsbehörde
- Imageverlust
- Schadensersatz von Betroffenen

Echt jetzt?!

Politische Aktivitäten der IHK im Datenschutz

- Große Betroffenheit gerade kleiner und mittelständischer Unternehmen
- Probleme bei der Anwendung des Rechtsrahmens
- Probleme bei der Umsetzung der Datenschutzanforderungen
- Verbotsprinzip hemmt wirtschaftliche aber auch wissenschaftliche Betätigung

Im Ernst?

- **30 Erforderlichkeitsprüfungen**

(Art. 5 Abs. 1c, Art. 5 Abs. 1d, Art. 6 Abs. 1b, c, d, e und f, Art. 7 Abs. 4, Art. 9 Abs. 2b, c, f, g, h, i und j, Art. 11 Abs. 1, Art. 13 Abs. 2, Art. 14 Abs. 2, Art. 17 Abs. 1 a, Art, 17 Abs. 3, Art. 21 Abs. 6, Art. 22 Abs. 2a, Art. 25 Abs. 2 Satz 1, Art. 34 Abs. 3a, Art. 49 Abs. 1b, c, d, e und f, Art. 49 Abs. 1 Satz 2)

- **13 Risikoprüfungen**

(Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 27 Abs. 2a, Art. 30 Abs. 5, Art. 32 Abs. 1 und 2, Art. 33 Abs. 1 Satz 1, Art. 34 Abs. 1, Art. 34 Abs. 3b, Art. 35 Abs. 1, Art, 36 Abs. 2, Art. 39 Abs. 2, Art. 49 Abs. 1a)

- **12 Angemessenheitsprüfungen**

(Art. 5 Abs. 1c, d und f, Art. 8 Abs. 2, Art. 12 Abs. 5a, Art. 15 Abs. 3 Satz 2, Art. 17 Abs. 2, Art. 22 Abs. 3, Art. 24 Abs. 2, Art. 33 Abs. 4)

- **11 Geeignetheitsprüfungen**

(Art. 5 Abs. 1 e, Art. 9 Abs. 2 d, Art. 12 Abs. 1 Satz 1, Art. 24 Abs. 1, Art. 24 Abs. 2, Art. 25 Abs. 1, Art. 25 Abs. 2 Satz 1, Art. 28 Abs. 1, Art. 28 Abs. 4, Art. 32 Abs. 1, Art. 34 Abs. 3a)

- **8 Interessenabwägungen**

(Art. 6 Abs. 1 f, Art. 15 Abs. 4, Art. 17 Abs. 1 c, Art. 17 Abs. 3, Art. 18 Abs. 1 d, Art. 20 Abs. 4, Art. 21 Abs. 1 Satz 2, Art. 49 Abs. 1 Satz 2)

- **3 Verhältnismäßigkeitsprüfungen**

(Art. 5 Abs. 1 c, Art. 14 Abs. 5b, Art. 19 Satz 1, Art. 34 Abs. 3c)

- **3 Treu- und Glauben bzw. Fairnessprüfungen**

(Art. 5 Abs. 1 a; Art. 13 Abs. 1, Art. 11 Abs. 2)

- **2 Vereinbarkeitsprüfungen**

(Art. 5 Abs. 1 b, Art. 6 Abs. 4)

Geht’s noch?!

16 x "Rechte"
50 x "Rechte und Freiheiten"
4 x "Rechte und Freiheiten sowie berechtigte Interessen"
1 x "Persönliche Rechte und Freiheiten"
1 x "Menschenrechte und Grundfreiheiten"
1 x "Rechte und berechtigte Interessen"
1 x "Datenschutzrechte"
3 x "Grundrechte"
13 x "Grundrechte und Grundfreiheiten"
3 x "Grundrechte und Interessen"
1 x "Grundrechte und Garantien"
1 x "Grundrechte und personenbezogene Daten"
1 x "Personenbezogene Daten und andere Grundrechte und Grundfreiheiten"
2 x "Interesse"
6 x "Berechtigte Interessen"
4 x "Zwingende berechtigte Interessen"
1 x. "Zwingende schutzwürdige Gründe"
6 x "Lebenswichtige Interessen"
1 x "Interessen und Rechte"
2 x "Interessen und Grundrechte"
1 x "Interessen, Rechte und Freiheiten"
2 x "Interessen oder Rechte und Freiheiten“
3 x "Interessen oder Grundrechte und Grundfreiheiten"
1 x "Menschliche Würde, berechtigte Interessen und Grundrechte"

Forderungen der Schleswig-Holsteinischen Wirtschaft zum Datenschutz

1. Das Datenschutzrecht darf unternehmerisches Handeln nicht unverhältnismäßig belasten.

2. Datenschutzregelungen müssen an der wirtschaftlichen Lebenswirklichkeit ausgerichtet sein. Das Verhältnis von Aufwand und Nutzen muss berücksichtigt werden.

3. Forschung und Entwicklung sind wichtiger Teil unternehmerischen Handelns. Datenschutzrechtliche Regelungen dürfen hier nicht behindern.

4. Die Datenschutzvorschriften müssen übersichtlich, verständlich, transparent und systematisch verfasst sein.

5. Ablösung des „one size fits all-Ansatz“ durch Berücksichtigung der Belange der KMU.

6. Datenschutzrechtliche Verpflichtungen müssen von der Größe des Unternehmens, der Komplexität der Datenverarbeitungsstrukturen, vom Umfang, dem Risiko und Qualität der Datenverarbeitung abhängig gemacht werden und nur dann zum Tragen kommen, wenn die Datenverarbeitung überraschend ist bzw. vom eigentlichen Geschäftsmodell abweicht.

7. Sämtliche vorhersehbare Datenverarbeitung aufgrund eines Vertrages, die gesetzlich verpflichtende Verarbeitung von Daten sowie eine Datenverarbeitung im Bagatellbereich darf keine Dokumentations-, Abwägungs-, Nachweis- oder Informationspflichten auslösen.

8. Es darf keine Wettbewerbsnachteile für deutsche Unternehmen geben, weil deutsches Recht über die EU-Anforderungen hinausgeht. Die Aufsichtsbehörden sollten einheitlich agieren mit klaren Zuständigkeiten und sich auch auf EU-Ebene abstimmen.

9. Eine anlassbezogene begründete Einzelfallprüfung durch die Aufsichtsbehörde ersetzt die umfassende Rechenschaftspflicht der Unternehmen. Bei der Auswahl der Verantwortlichen im Falle der Inanspruchnahme durch die Aufsichtsbehörde muss die Effektivität bei der Bekämpfung von Datenschutzverstößen im Vordergrund stehen.

10. Unternehmen brauchen von den datenschutzrechtlichen Aufsichtsbehörden unterstützende praxisnahe lösungsorientierte Beratung (verbindliche Guidance) auch durch Checklisten, Mustervorgaben und konstruktive Hinweise, um Rechtsunsicherheiten und Haftungsrisiken zu vermeiden.

Politische Aktivitäten der IHK im Datenschutz

- Echten Mehrwert bieten
- Konkrete Änderungen vorschlagen
- Verbündete finden
- Evaluierung der DSGVO in 2024 nutzen
- Änderungen im BDSG und LDSG einfordern

- Wir bleiben am Ball, versprochen!

Vielen Dank

für Ihre

Aufmerksamkeit!