Die Datenschutzbeauftragten vor Ort – Vorsorge ist besser als Nachsorge

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

Wien, 22.10.2019

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- EU-weit neu mit der DSGVO (und JI-Richtlinie): Datenschutzbeauftragte (bDSB)
- Rolle der/des bDSB
- Aufgaben der/des bDSB
  - Einsatz vor Ort
  - Von Vorsorge bis Nachsorge
- Fazit

Alles neu? Betriebliche und behördliche Datenschutzbeauftragte

- Nicht (überall) so neu
- Aber in der Entstehung der DSGVO kein Selbstgänger

- Geregelt:
  - Artikel 37 ff. DSGVO
  - Artikel 32 ff. JI-RL (Richtlinie (EU) 2016/680)
  - § 5 DSG (Ö) //
    §§ 5 ff. sowie § 38 BDSG (D)

- Behördlich als Muss [Art. 37 (1) a DSGVO]
- Betrieblich bei bestimmten Bedingungen [Art. 37 (1) b+c DSGVO, Art. 37 (4) DSGVO]

Wann in Deutschland?

Benennungspflicht gemäß § 38 BDSG

Wenn

- in der Regel mindestens 10 (künftig: 20) Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden, oder
- Verarbeitungen vorliegen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder
- unabhängig von der Anzahl beschäftigter Personen geschäftsmäßige Verarbeitung zum Zweck
  - der Übermittlung,
  - der anonymisierten Übermittlung oder
  - für Zwecke der Markt- oder Meinungsforschung

Überblick

Bild: silviarita via Pixabay

- EU-weit neu mit der DSGVO (und JI-Richtlinie): Datenschutzbeauftragte (bDSB)
- Rolle der/des bDSB
- Aufgaben der/des bDSB
  - Einsatz vor Ort
  - Von Vorsorge bis Nachsorge
- Fazit

Rolle bDSB – Sicht 1: „Klar, bDSB soll haften“?

Bild: Tumisu via Pixabay

- *„Einer macht bei uns den Datenschutz, das reicht dann auch – oder?“*
- bDSB als Sündenbock, wenn es schiefgeht?
- Aber: verantwortlich ist der Verantwortliche!

Rolle bDSB – Sicht 2: „für die Betroffenen da“?

Bild: Edward Lich via Pixabay

- bDSB als „Anwalt“ der Betroffenen?
- *„Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.“* [Art. 38 (4) DSGVO]
- Sicht der Betroffenen einnehmen

Rolle bDSB – Sicht 3: „eierlegende Wollmilchsau“?

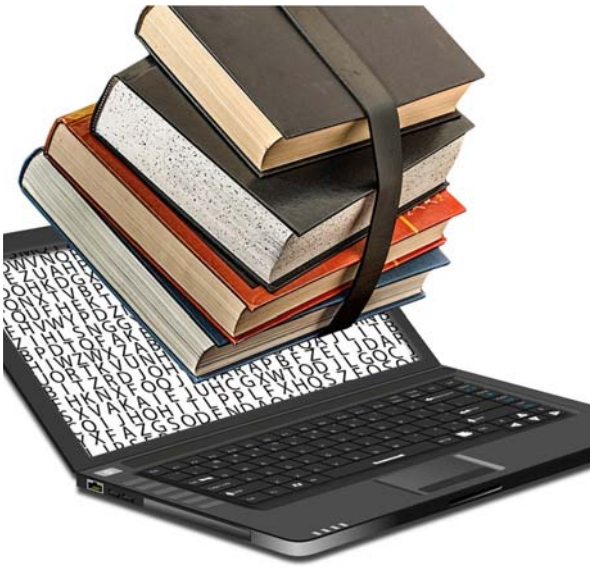

Bild: Gerd Altmann via Pixabay

- bDSB als Super-Experte
- *„Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.“* [Art. 37 (5) DSGVO]

Rolle bDSB – Sicht 4: „Feuermelder“?

Bild: Antranias via Pixabay

„Die Datenschutzbeauftragten sind wie Feuermelder, die Kontrollbehörden wie die Feuerwehr.“
– Andrea Voßhoff, 2015

- Warner?
- Gar Whistleblower gegenüber den Aufsichtsbehörden++?
- Aber: zum Verantwortlichen gehörig

Rolle bDSB – Sicht 5: „die Säule neben der Aufsichtsbehörde“?

Bild: Free-Photos via Pixabay

- bDSB als eine Säule in einem Zwei-Säulen-Modell
- Neben der Aufsichtsbehörde
- Aber: auch vor Ort Trennung operativ / prüfend

Rolle bDSB – Sicht 6: Teil des Datenschutz-Managementsystems

Bild: kalhh via Pixabay

- bDSB als eine Säule in einem Mehr-Säulen-Modell
- DSMS:
  - Mit Team für operativen Datenschutz / DS-Koord.
- Parallel zu IT-Sicherheitsmgt.
- Gemeinsame Jour fixes
- bDSB als Stabsstelle [Art. 38 (3) DSGVO]
- Interessenkonflikte vermeiden! [Art. 38 (6) DSGVO]

Wenn Anzeichen: Rolle bDSB?

Überblick

Bild: silviarita via Pixabay

- EU-weit neu mit der DSGVO (und JI-Richtlinie): Datenschutzbeauftragte (bDSB)
- Rolle der/des bDSB
- Aufgaben der/des bDSB
  - Einsatz vor Ort
  - Von Vorsorge bis Nachsorge
- Fazit

Über welche Zahlen sprechen wir?

Quelle: iapp.org

- IAPP:
  - Ca. 500.000 Organisationen benötigen einen bDSB
  - Im Sommer 2019 ca. 375.000 Meldungen von bDSB
- Schleswig-Holstein:
  - Ca. 8.000 Meldungen
  - Vielfach gemeinsame bDSB
  - Für öffentlichen Dienst Daumenregel in S-H:
    1 bDSB für nicht mehr als 1.000 Beschäftigte

Highlander-Prinzip

 Bild: tommy pixel via Pixabay

- „Es kann nur einen geben.“ (D)
- Besondere Rechte der/des bDSB:
  - Prüf- / Zugriffsrechte
  - Keine Benachteiligung [Art. 38 (3) DSGVO]
  - Kündigungsschutz (D) [§ 6 (4) BDSG]
  - Weisungsfrei [Art. 38 (3) DSGVO]
- Vertretung? Operativ ohnehin andere
- Auch juristische Person?
  In D: natürliche Person

Aufgaben *[Art. 39 DSGVO]*

Bild: stux via Pixabay

- Unterrichtung und Beratung der Organisation (Leitung + Beschäftigte) [Buchst. a]
- Sensibilisierung und Schulung [b]
- Überwachung DS-Rechts-konformität inkl. Überprüfung [b]
- Beratung DSFA [c]
- Zusammenarbeit mit Aufsichtsbehörde [d]
- Anlaufstelle für Aufsichtsbehörde (u.a. vorherige Konsultation) [e]
- Dokumentation und Bericht über bDSB-Tätigkeit

Dafür notwendig

Bild: Alexas Fotos via Pixabay

- Prozesse für Einbindung [Art. 38 (1) DSGVO]
  - *„ordnungsgemäß und frühzeitig“*
  - *„in alle […] Fragen“*
- Ressourcen [Art. 38 (2) DSGVO]
  - *„für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu pb Daten und Verarb.vorgängen“*
  - Fachwissen erhalten
- Verantwortlicher / Auftragsverarbeiter *„stellt sicher, […]“* [Art. 38 DSGVO]

Finanziell, räumlich, technisch ...

Austausch

Rolle bDSB?

Von Vorsorge bis Nachsorge

- Datenschutzmanagement [s.a. Art. 5 Abs. 2 DSGVO, Art. 24 DSGVO, Art. 25 DSGVO, ...]
- Abstimmung mit Sicherheitsmanagement (ISMS)
  [s.a. Art. 32 DSGVO]
- Beschäftigte sensibilisieren (mehr als Art. 29 DSGVO oder „Datengeheimnis“)
- Risiko-Einschätzung schon bei Gestaltung der Systeme
  [Art. 32 + Art. 35 DSGVO]
- Beratung durch bDSB bei Meldeprozess für Datenpannen
  [Art. 33 + Art. 34 DSGVO]
- Anlassbezogene und anlasslose interne Prüfungen
- Perspektive: betroffene Personen intern und extern

Aber bDSB mit anderer Perspektive

Risiko – nicht nur Sicherheitsperspektive

- Risiko für die Rechte und Freiheiten natürlicher Personen
- D.h. mehr als „nur“ Datensicherheit
- Definiert durch die Eintrittswahrscheinlichkeit und die Schwere eines möglichen Schadens (siehe EG 75)
- In Bezug auf Art, Umfang, Umstände und Zwecke der Verarbeitung; objektive Bewertung gefordert (siehe EG 76)
- Physischer, materieller oder immaterieller Schaden (siehe EG 75+85)

Beispiele aus EG 85:
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- Finanzielle Verluste
- Unbefugte Aufhebung der Pseudonymität
- Rufschädigung
- Erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Beispiele für besondere bDSB-Aktionen

Bild: Dimitris Vetsikas via Pixabay

bDSB: vom Prüfer bis zum Motivationstrainer

- Aktionstag „Löschen/Schreddern“
- Datenschutz-Gamification mit Preis (Obst/Schokoriegel)
- Datenschutz-Quiz
- Datenpannen-Simulation
- Szenario-Technik bei Risiko/DSFA
- Schulung der Mitarbeitenden mit Mehrwert (Selbstdatenschutz)
- Phishing-Test (anonym realisiert)
- Im Team produzierte Kurzvideos für Schulungszwecke

Überblick

Bild: silviarita via Pixabay

- EU-weit neu mit der DSGVO (und JI-Richtlinie): Datenschutzbeauftragte (bDSB)
- Rolle der/des bDSB
- Aufgaben der/des bDSB
  - Einsatz vor Ort
  - Von Vorsorge bis Nachsorge
- Fazit

Fazit

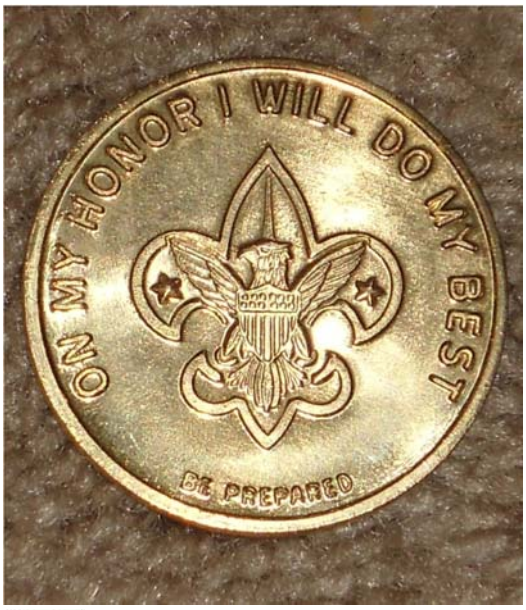

Bild: jclovis3 via Pixabay

- bDSB als *ein* wesentliches Instrument für Datenschutz
- Vorsorge ist besser als Nachsorge
  - Technisch-organisatorische Maßnahmen (mit ISMS)
  - Aufmerksame und sensibilisierte Beschäftigte (z.B. Notfallkarte)
  - Prüfen + Ernstfall proben
- Vertrauensvolle Zusammenarbeit auch mit Aufsichtsbehörde

Und Ihre Fragen?

Marit Hansen
https://www.datenschutzzentrum.de/