Roland Breda
Unternehmensberatung externer Datenschutzbeauftragter

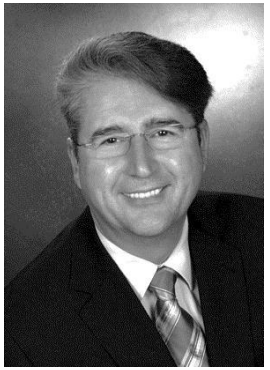
Die DSGVO gilt seit dem 25.05.2018 – Was muss ich alles erledigen?

3. Wachstumsabend

Dienstag, 22. Januar 2019

Roland Breda
Unternehmensberatung externer Datenschutzbeauftragter

Ihr externer Datenschutzbeauftragter



Roland Breda, Dipl.-Kfm. (RWTH Aachen)

u. a. Erfahrungen als HR Manager (international), KAIZEN Trainer, NLP-Ausbildung, RProfile Master, ehrenamtlicher Richter am Sozialgericht Aachen bzw. Arbeitsgericht Heinsberg

DSB Zertifizierung durch UDIS

Gibt es einen „Fahrplan“ für die Umsetzung der DSGVO?

VdS 10010 – Richtlinie zur Einführung der DSGVO

VdS 3473 – Cyber Security für KMU

VdS 10000 – ISMS für KMU

Man kann sich anhand dieser Richtlinien orientieren, aber sich auch zertifizieren lassen

Die Richtlinien können Sie kostenlos von der Homepage der VdS downloaden.

https://vds.de/de/richtlinien/nummerische-liste/

Wie kann ich eine „Standortbestimmung“ durchführen

Auf der Homepage „www.vds-quick-check.de“
finden Sie die Möglichkeit Ihr Unternehmen im Hinblick auf
die folgenden drei Bereiche kostenlos selber zu analysieren

- Quick Check für Datenschutz gemäß DSGVO
- Quick Check für Cyber Security
- Quick Check für ICS

- https://www.vds-quick-check.de/

Was erwartet der Landesdatenschutz-beauftragte NRW von mir?

✓ Wesentliche DS-GVO-Anforderungen für den Online-Shop

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom Online-Shop benannt werden?
☐ ja
☒ nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
☐ nein

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
☒ ja (bei den Mitarbeitern, die mit personenbezogenen Daten umgehen)
☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
☒ ja (insb. auf der Webseite in der Datenschutz-erklärung sowie bei Vertragsabschluss)
☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
☒ ja (insb. der Kundendaten, aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
☒ ja (die auf der Webplattform verarbeiteten Daten müssen vor Angriffen geschützt werden)
☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
☒ ja (mit dem Hosting-Anbieter, dem Lohnabrechner und dem Zahlungsdienstleister)
☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
☒ ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Muss eine DSFA vom Verein durchgeführt werden?
☐ ja
☒ nein (da kein hohes Risiko bei der Daten-verarbeitung im Betrieb besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☐ ja
☒ nein (da keine Videoüberwachung vom Unternehmen durchgeführt wird)

https://www.lda.bayern.de/de/kleine-unternehmen.html

Roland Breda
Unternehmensberatung externer Datenschutzbeauftragter

Gibt es bereits Kontrollen?

Datenschutzprüfungen	
12/2018	
Löschen von Daten bei ERP-Systemen (SAP)	Status: Anstehend
11/2018	
Datenschutzverletzungen bei (Unter-)Auftragverarbeitern	Status: Anstehend
Patch Management WordPress – WP GDPR Compliance Plugin	Status: Läuft
Umsetzung der DS-GVO bei kleinen und mittelständischen Unternehmen (KMUs)	Status: Läuft
10/2018	
Patch Management eCommerce-Systeme/Online-Shops (Magento)	Status: Läuft
Informationspflichten in Bewerbungsverfahren	Status: Läuft
Ransomware bei Arztpraxen	Status: Läuft
Rechenschaftspflicht bei Großkonzernen	Status: Läuft
02/2018	
Patch Management Content Management Systeme (WordPress)	Status: Abgeschlossen

https://www.lda.bayern.de/de/kontrollen.html

Was muss ich hinsichtlich der Bestellung eines DSB beachten?

Zu prüfen ist eine Bestellungspflicht eines DSB nach:

- Art. 37 DSGVO
- § 38 BDSG n. F.

Es kann auch freiwillig ein DSB benannt werden

Im Fall einer Benennung muss der zuständige Landesdatenschutzbeauftragte informiert werden. Bei einer verspäteten Meldung haben die LDB bis zum 31.12.2018 keine Bußgelder verhängt.

Was muss ich hinsichtlich der Homepage meines Unternehmens beachten?

Korrekte Informationen müssen zu diesen Bereichen vorhanden sein:

- Impressum (§ 5 TMG)
- Datenschutzerklärung (§ 13 TMG)
- Datenschutzinformationen (Art. 13/14 DSGVO)
  https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Informationspflichten-nach-der-Datenschutz-Grundverordnung/Umsetzungshilfe-Datenschutzinformationen_Stand-01_2019.pdf

Was muss ich bezüglich meiner Prozesse dokumentieren?

- Zu jedem Verfahren, in dem pbD verarbeitet werden muss ein Verfahrensverzeichnis erstellt werden
- Gehört zu den Rechtsgrundlagen des Verfahrens eine Interessenabwägung, muss diese dokumentieren werden
- Für jedes Verfahren muss eine Risikoabwägung erstellen werden
- Stellt sich heraus, dass das Risiko des Verfahrens „hoch“ ist, muss eine DSFA erstellt werden
- Jedes Verfahren muss von der verantwortlichen Person in der Organisation jährlich auf Änderungen geprüft und ggf. angepasst werden
- Werden TOM´s für jedes Verfahren dokumentiert oder wurde ein „Datenschutzkonzept“ für das Unternehmen erstellt?

Was muss ich tun, wenn die Verfahren outgesourced werden?

Wenn Externe pbD meines Unternehmens verarbeiten, muss ich:

- prüfen, ob eine Auftragsverarbeitung vorliegt
- Wenn ja muss ich prüfen, ob der Auftragsverarbeiter in der Lage ist, die Anforderungen der DSGVO zu erfüllen
- Einen Auftragsverarbeitungsvertrag mit dem Auftragsverarbeiter abschließen
- Die durch den Dienstleister offengelegten TOMS´s prüfen
- Regelungen treffen, wie ich über ggf. hinzugezogene Unterauftragsnehmer mitbestimme
- Regelungen treffen, wie Dienstleister aus Drittländern das erforderliche Datenschutzniveau garantieren
- Für den Fall „Joint Controller“ rechtssichere Regelungen treffen
- www.lda.bayern.de/media/muster_adv.pdf

Habe ich den Text der Einwilligungs-erklärungen an die DSGVO angepasst?

- Ist der allg. Text rechtssicher?
- Wurde das Recht am Bild berücksichtigt?

- Berücksichtigt das Kontaktformular der Homepage die Einverständniserklärung mit der Verarbeitung der Anfrage?

Habe ich meine Mitarbeiter auf die Vertraulichkeit verpflichtet?

Habe ich Regelungen für die Rechte der betroffenen Personen festgelegt?

Art. 12: Transparente Information
Art. 13: Informationspflicht
Art. 14: Informationspflicht
Art. 15: Auskunftsrecht
Art. 16: Recht auf Berichtigung
Art. 17: Recht auf Löschung
Art. 18: Recht auf Einschränkung der Verarbeitung
Art. 19: Mitteilungspflicht in zus. mit Berichtigung/Löschung
Art. 20: Recht auf Datenübertragbarkeit
Art. 21: Widerspruchsrecht
Art. 22: automatisierte Entscheidungen
Art. 23: Beschränkungen

https://www.lda.bayern.de/de/dsk.html

Königsdisziplin „Löschkonzept“

Ein Löschkonzept wird nach der DSGVO durch Art. 17 gefordert.

Mit der DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ liegt eine Vorschrift zur Umsetzung dieser schwierigen Thematik bereits vor.

Haben Sie ein DS-Handbuch erstellt?

Mit den einzelnen Richtlinien:

- Leitlinie zu DS und IS
- Richtlinie zum DS für Beschäftigte
- RL zur Umsetzung von DS Maßnahmen
- Grundsätze zur Einrichtung und Änderungen von Verarbeitungen mit pbD
- RL für die Umsetzung von Betroffenenrechten
- IT RL für Nutzer
- RL für Speicherorte
- RL für die Nutzung mobiler IT-Systeme
- RL für die Nutzung mobiler Datenträger
- RL Regelungen für Lieferanten und sonstige Auftragsnehmer
- RL für Störungen und sonstige Ausfälle
- RL für Sicherheitsvorfälle
- Notfallplan

Organisation

Haupt-Aufgaben des Unternehmens	Etablierung • Datenschutz-Management (insbesondere im Hinblick auf „Accountability“/ Rechenschaftspflicht) • IT-Sicherheitsmanagement
Haupt-Aufgaben der Fachabteilung, Mitarbeiter	Umsetzung • Prozess-Inventur (Aufnahme aller Prozesse -> Verzeichnis von Verarbeitungstätigkeiten) • Prozessgestaltung (Privacy by Design/ Default) • Datenschutz-Folgenabschätzung/ PIA • Dokumentationen/ Nachweise/ Meldepflichten • Prozesse für Rechte der Betroffenen

Organisation

Datenschutzbeauftragter (DSB)	Bestellung/ Stellung • Bestellpflicht nach deutschem Recht (neues BDSG) bleibt • Bestandteil des Datenschutz-Managements
Haupt-Aufgaben des DSB	• Risikoorientierte Aufgabenerfüllung (berücksichtigt die Art, den Umfang, die Umstände, und die Zwecke) • Berichts-, • Beratungs-, • Kontroll- • und Kooperationsaufgaben

Wohin wir unsere Organisation entwickeln müssen