Datenschutz im Unternehmen

Erich Zimmermann

Externer Datenschutzbeauftragter (IHK)

Sprecher der Initiative „Sicherheit mit System“

ZiDa
Datenschutz GmbH

SIMIS Sicherheit mit System
Geprüfter Datenschutz
SIMIS DATA
PRÜFSIEGEL

e.zimmermann@zida-datenschutz.de

www.zida-datenschutz.de

Datenschutz im Unternehmen

Es ist höchste Zeit, in Sachen Datenschutz zu handeln! Es sei denn…

1. Sie haben keine Mitarbeiter/innen
2. Sie akzeptieren keine EC-Karten, Kreditkarten etc. (nur anonymer Barverkauf)
3. Sie sind nicht im INTERNET präsent (Homepage)
4. Sie versenden keine Werbemails

Ab 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung (EU-DSGVO)

u.a. neu : Meldepflicht bis spätestens 24.Mai 2018 der Kontaktdaten des ordnungsgemäß (ausgebildeten und unabhängigen) - beim Unternehmen bestellten Datenschutzbeauftragten - an die jeweilige Landesdatenschutzbehörde - mit entsprechend folgenden Sanktionen bei Nichtmeldung (siehe folgende Aussagen der Landesdatenschutzbehörde Baden-Württemberg).

Erweiterte Dokumentationsvorschriften und Maßnahmen für jedes Unternehmen - unabhängig von der Größe.

Bußgelder bis 2 % vom Jahresumsatz bzw. 20 Mio. Euro
(bisher max. 50.000 Euro) in extremen Fällen bis 40 Mio. Euro !

Interner Datenschutzbeauftragter kann zukünftig u.U. mithaften.

Aussagen der Landesdatenschutzbehörde Baden-Württemberg vom 31.08.17 zur Meldepflicht (1)

Antwort der Landesdatenschutzbehörde Baden-Württemberg, Stuttgart vom 31.08.2017 auf unsere Fragen zur zukünftigen Meldepflicht (ab 25.Mai 2018) der Kontaktdaten des bestellten Datenschutzbeauftragten der verantwortlichen Stelle, also dem Unternehmen.

1) ob die neue Meldepflicht der Kontaktdaten des bestellten Datenschutzbeauftragten für alle Unternehmen gilt ?

2) wohin muss gemeldet werden ?

3) auf welche Art muss gemeldet werden ?

4) welche Sanktionen der Behörde drohen bei Nichtbefolgung ?

Aussagen der Landesdatenschutzbehörde Baden-Württemberg vom 31.08.17 zur Meldepflicht (2)

1) ob die neue Meldepflicht der Kontaktdaten des bestellten

Datenschutzbeauftragten für alle Unternehmen gilt ?

Zu 1.: Ja, diese Regelung gilt für alle verantwortlichen Stellen* bzw. Auftragsverarbeiter. ***Anmerkung Unternehmen**

Aussagen der Landesdatenschutzbehörde Baden-Württemberg vom 31.08.17 zur Meldepflicht (3)

2) wohin muss gemeldet werden ?

Zu 2.: Die Informationspflicht gilt gegenüber der örtlich zuständigen Datenschutzaufsichtsbehörde, also gegenüber dem Landesdatenschutzbeauftragten, in dessen Land die verantwortliche Stelle bzw. der Auftragsverarbeiter seinen Hauptsitz hat.

3) auf welche Art muss gemeldet werden ?

Zu 3.: Die Landesdatenschutzbeauftragten arbeiten derzeit an einer Onlinelösung für die Meldung. Näheres werden Sie rechtzeitig auf unserer Internetseite erfahren.

Aussagen der Landesdatenschutzbehörde Baden-Württemberg vom 31.08.17 zur Meldepflicht (4)

4) welche Sanktionen der Behörde drohen bei Nichtbefolgung ?

zu 4.: Die unterlassene Meldung stellt einen Bußgeldtatbestand nach Art. 83 Absatz 4 Buchstabe a EU-DSGVO dar, der eine Geldbuße bis zu 10 Mio. Euro oder bis zu 2 % des weltweit erzielten Jahresumsatzes zur Folge haben kann.

Erfordernisse der Datenschutz-Gesetzgebung BDSG bzw. EU-DSGVO

- Ein betrieblicher (interner oder externer) Datenschutzbeauftragter muss bestellt werden, wenn - abhängig von der Beschäftigtenzahl (Köpfe) -

  ab 10 Arbeitnehmer/innen (GF, Teilzeitkräfte / Aushilfen zählen voll) mit automatisierter Datenverarbeitung (auch Kassenplätze, e-Mail-Adressen, Firmen-Handy etc. zählen) im Unternehmen beschäftigt sind;

- Unabhängig von der Zahl der Beschäftigten,
  (also auch Unternehmen kleiner 10 Personen) wenn z.B.
  - Videoüberwachung stattfindet (siehe § 4f BDSG)
  - sensible, risikobehaftete Daten (Finanzierung, Gesundheitsdaten etc...) erfasst werden.

  Wichtig: Es drohen hohe Bußgelder - gemäß neuer EU-DSGVO

  bis 10 Mio. Euro bzw. 2 % vom Jahresumsatz, in extremen Fällen bis 20 Mio. Euro oder 4 % vom Jahresumsatz.

Fragebogen zur EU-DSGVO (1)

// Gibt es das Bewusstsein im Unternehmen dass Datenschutz Chefsache ist, beispielsweise durch:

- Vorhandensein einer Datenschutzleitlinie
- Beschreibung der Datenschutzziele
- Regelung der Verantwortlichkeiten
- Bewusstsein der Datenschutzrisiken

// Ist Datenschutzbeauftragter vorhanden und ist er schon der Aufsichtsbehörde gem. Art.37 DS-GVO gemeldet ?

Fragebogen zur EU-DSGVO (2)

- Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten ?
- Wie stellen Sie sicher, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen berücksichtigt werden ?

Fragebogen zur EU-DSGVO (3)

- Haben Sie EXTERNE zur Erledigung Ihrer Arbeiten eingebunden (Auftragsverarbeiter) ?
- Haben Sie hierüber eine Übersicht ?
- Haben Sie die erforderlichen Vereinbarungen zum Datenschutz / Geheimhaltung ..abgeschlossen ?

Fragebogen zur EU-DSGVO (4)

- Zur Transparenz, Informationspflicht und Sicherstellung der Betroffenenrechte:
- Kontaktdaten des Datenschutzbeauftragten
- Berücksichtigung der Rechte Betroffener auf Auskunft, Berichtigung, Löschung, Sperrung..
- Verfahren eingerichtet, um Anträge auf Auskunft zeitnah erfüllen zu können
- Widerrufsrecht bei Einwilligung (Werbung..)

Fragebogen zur EU-DSGVO (5)

- Gibt es zu den Verarbeitungstätigkeiten Angaben, mit denen die Rechtmäßigkeit nachgewiesen werden kann, z.B. Zweck, Kategorien, Empfänger, Löschfristen ?
- Können Einwilligungen (Werbung..) nachgewiesen werden ?

Fragebogen zur EU-DSGVO (6)

- Haben Sie eine Risikobewertung mit Eintrittswahrscheinlichkeit und Schwere der Risiken mit regelmäßiger Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen eingerichtet ?
- Ist ein Prozess zur Datenschutz-Folgenabschätzung (Risikomethode ähnlich ISO 27001-Informationssicherheit) etabliert ?
-

Fragebogen zur EU-DSGVO (7)

- Haben Sie sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörden und die Betroffenen erfolgt ?
- Ist festgelegt, wie diesbezüglich mit potentiellen Verletzungen intern umzugehen ist (Meldeverfahren, Informationsweg..) ?

Erfordernisse der Datenschutz-Gesetzgebung

Jedes Unternehmen muss Datenschutz umsetzen!

Beispiele von Vorkommnissen aus der Praxis (1):

1. Kunde, Anwalt, Abmahnverein,Wettbewerber.. erkundigt sich gemäß § 34 BDSG (Betroffener) nach dem Datenschutz in Ihrem Unternehmen (siehe folgender Musterbrief..) – Absicht oft – finanziell (Nachlass auf Kaufpreis, Anwaltsgebühren, schädigen..)

Erfordernisse der Datenschutz-Gesetzgebung

Jedes Unternehmen muss Datenschutz umsetzen!

weitere Beispiele von Vorkommnissen aus meiner Praxis :

2. Landesdatenschutz-Behörde sendet Fragebogen bzw. ordnet eine Überprüfung des Unternehmens vor Ort an (siehe Fragebogenaktion ausgewählte Unternehmen in Rheinland-Pfalz, Hamburg, Bayern - Zufallsprinzip bzw. gezielt).
3. Datenschutzvorfall (z.B. unerlaubte Werbepost, eMail etc.) führt nach Anzeige des Betroffenen zur Überprüfung des Unternehmens durch die Landesdatenschutzbehörde (Datenschutzbeauftragter erforderlich und ausgebildet vorhanden, Richtlinien verabschiedet, Personal im Datenschutz geschult, externe Dienstleister im Datenschutz verpflichtet, Regelung zur Videoüberwachung vorhanden ..usw. ? mit entspr. Folgen u.a. Bußgeld etc.)

zu vorgenannten Vorkommnissen aus der Praxis (1):

Musterschreiben (Betroffenen-Anfrage) nach BDSG, das jederzeit bei Ihnen eintreffen kann (per Einschreiben, per eMail, per Fax ..)

Sehr geehrte Damen und Herren,

unter Bezug auf § 34 BDSG ersuche ich Sie, mir schriftlich, unverzüglich und kostenlos Auskunft über die zu meiner Person bei Ihnen gespeicherten Informationen zu erteilen :

Werden in Ihrem Unternehmen Daten über mich gespeichert ?

Welche Daten zu meiner Person werden gespeichert ?

Wer verarbeitet die Daten ?

Von wem haben Sie Ihre Daten über meine Person erhalten (Quelle) ?

Zu welchem Zweck werden die Daten verarbeitet ?

An welche weiteren Empfänger wurden in der Vergangenheit meine persönlichen Daten weitergegeben ?

Nennen Sie mir Ihren Datenschutzbeauftragten und dessen Kontaktdaten.

Bitte erteilen Sie mir Auskunft bis zum TT.MM.JJJJ. Mit freundlichen Grüßen

Bestellung eines Datenschutzbeauftragten (DSB) interner - betrieblicher - DSB

- // Inhaber - Geschäftsführer und deren Angehörige sowie IT-Mitarbeiter/innen können nicht zum DSB bestellt werden
- // Keine Weisungsbefugnis der Geschäftsleitung - freie Zeiteinteilung des DSB für die Datenschutzaufgaben - Fachliteratur - Budget..
- // Individuelle, lfd. Ausbildungskosten zum DSB ohne branchenspezifische Vorlagen (juristische Kenntnisse, fundierte IT-Kenntnisse usw.)
- // Hoher Kündigungsschutz - auch noch 1 Jahr nach Abberufung
- // Geschäftsführung haftet weiter - und neu mit EU-DSGVO - ggf. Mithaftung des internen DSB

Die Lösung;
der externe Datenschutzbeauftragte (DSB) - Vorteile:

- Flexibilität: unterliegt keinem besonderen Kündigungsschutz – im Gegensatz zum eigenen, betrieblichen DSB
- Branchenspezifische Vorlagen vorhanden, daher geringer Aufwand für den Kunden bei der Einführung der Datenschutz-Dokumentation, Kunde benötigt keinen eigenen MA für den Datenschutz
- Professionell, keine zusätzlichen Kosten für Aus- und Weiterbildung
- Minimiert Haftungsrisiken
  - Geschäftsführer haftet persönlich für Fehler oder Versäumnisse im Datenschutz - haftet bei internem DSB (u.U. haftet dieser mit)
- Der externe Datenschutzbeauftragte haftet umfänglich
  - auch für Bußgelder (bei ZiDa über spezielle Haftpflichtversicherung abgedeckt)
  - sein Dienstleistungsvertrag ist befristet und seine Kernkompetenz ist der Datenschutz

Jedes Unternehmen muss den Datenschutz umsetzen !

Was ist generell zu tun ?

Inhalte der Datenschutzdokumentation (gesetzlich vorgeschrieben) für Unternehmen jeder Größe - unabhängig von der Bestellung des DSB - :

1. *Verzeichnis von Verarbeitungstätigkeiten ggf. mit Risikobeurteilung*
2. *Richtlinien u.a. Internet (email) und IT-Nutzung*
3. *Verpflichtung Personal und externer Dienstleister mit Zugriffsmöglichkeit auf personenbezogene Daten (Auftragsdatenverarbeiter – ADV)*
4. *Schulung des Personals in Datenschutz*
5. *Technische und organisatorische Maßnahmen zur Vermeidung von Datenschutzvorfällen*

ZiDa hat fertige Datenschutz-Vorlagen für Ihre Branche.

Diese werden jeweils durch ZiDa mit sehr geringem Aufwand für den Kunden vor Ort individuell angepasst.

Professioneller Datenschutz !
Wo stehen Sie ?

Kostenloser Datenschutz-Check

Nehmen Sie sich ca. 30 Minuten Zeit und bearbeiten Sie mit uns - telefonisch (ggf. bei Ihnen) und vertraulich - Fragen zum Datenschutz-Status in Ihrem Unternehmen anhand einer „Datenschutz-Checkliste“.

Sie erhalten dann kostenlos Hinweise zu den für Ihr Haus zutreffenden Datenschutz- und Informations-Sicherheits-Erfordernissen und können Ihr persönliches Risiko besser einschätzen.

Bitte fordern Sie den kostenlosen Check bei uns an:

Tel. 0621 - 30696731 bzw. Fax: 03212 - 3912345

eMail: info@zida-gmbh.de

„Prüfsiegel -
Datenschutz als Qualitätsmerkmal und Wettbewerbsvorteil“

Checkliste der wichtigsten Änderungen durch die EU-Datenschutz-Grundverordnung(EU-DSGVO ab Mai 2018)-1-

- Drastisch erhöhte Bußgelder: bis zu vier Prozent des globalen Umsatzes bzw. 20 Mio. Euro

- Persönliche Haftung der Geschäftsführung bei Nichtbestellung des Datenschutzbeauftragten (DSB)

- Deutlich erweiterte zivilrechtliche Haftung: Ersatz auch immaterieller Schäden, Beweislastumkehr..

- Stellung des Datenschutzbeauftragten:
  Zusätzliche Verantwortung und Haftung für DSB (auch interner)

- Stark erweiterte Dokumentations- und Nachweispflichten

- Datenschutz-Folgenabschätzung statt Vorabkontrolle:
  Weitergehende Prüf- und Abstimmungspflichten (PDCA)

Checkliste der wichtigsten Änderungen durch die EU-Datenschutz-Grundverordnung (EU-DSGVO ab Mai 2018) -2

- Risikobasierter Datenschutz (Risk-/Compliance)
- Globale Anwendung der DSGVO möglich
- Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen
- Erweiterte Melde und Benachrichtigungspflichten bei Datenschutzverstößen
- Striktere Löschpflichten und Recht auf Vergessenwerden
- Erleichterter Datenaustausch im Konzern
- Koppelungsverbot bei Einwilligungen
- Erhöhte Haftung des Auftragsdatenverarbeiters (gesamtschuldnerisch)

Erich Zimmermann

Sprecher der Initiative „Sicherheit mit System“

externer Datenschutzbeauftragter (IHK)

ZiDa-Datenschutz GmbH, Waldhofer Str. 102, 69123 Heidelberg

Tel. 0621 - 30696731

Fax. 03212 - 3912345

e.zimmermann@zida-datenschutz.de

www.zida-datenschutz.de