DATENSCHUTZ IM UNTERNEHMEN

bm-Netzwerktreffen
am 26. September 2024

BEGRIFFLICHKEITEN ZUM DATENSCHUTZ

PETER STEFFKE
Managementberatung

Wann müssen wir uns mit dem Datenschutz beschäftigen?

- Bei der Verarbeitung
- personenbezogener Daten von natürlichen Personen

BEGRIFFLICHKEITEN ZUM DATENSCHUTZ

PETER STEFFKE
Managementberatung

- Verarbeitung (Art. 4 DSGVO)

„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“

BEGRIFFLICHKEITEN ZUM DATENSCHUTZ

PETER STEFFKE
Managementberatung

- personenbezogene Daten (Art. 4 DSGVO)

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“

REGELUNGEN ZUM DATENSCHUTZ

PETER STEFFKE
Managementberatung

- EU-Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Betriebsverfassungsgesetz (BetrVG)
- Handelsgesetzbuch (HGB) und Abgabenordnung (AO)
- Gesetz gegen den unlauteren Wettbewerb (UWG)
- Telekommunikations-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)
- EU-U.S. Data Privacy Framework

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

Data Act

- Am 27. November 2023 hat der Rat der Europäischen Union die „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“ (kurz: Data Act) verabschiedet.
- Der Data Act ist am 11. Januar 2024 in Kraft getreten und wird nach einer grundsätzlichen Übergangsfrist von 20 Monaten ab dem 12. September 2025 EU-weit direkt anwendbares Recht werden.
- Der Data Act ergänzt die DSGVO und fokussiert sich auf nicht-personenbezogene, datennutzergenerierte Daten.

Quelle: www.bmdv.bund.de

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

Data Act

- Daten besser nutzbar machen – der Data-Act soll für alle Akteure in der wirtschaftlichen Wertschöpfungskette den Austausch und die Nutzung von Unternehmensdaten verbessern beziehungsweise überhaupt erst ermöglichen.
- Enthalten sind Regelungen für die Nutzung von Daten zwischen Unternehmen (B2B), zwischen Unternehmen und Verbrauchern (B2C) und zwischen Unternehmen und Behörden (B2G).
- Betroffen sind insbesondere Hersteller, Dateninhaber und Nutzer von vernetzen Geräten, zum Beispiel Haushaltsgeräten, Maschinen oder Autos. Darüber hinaus werden auch auf Anbieter von Datenverarbeitungsdiensten, etwa Cloud-Anbieter, neue Pflichten zukommen.
- Konkret sieht der Data Act vor, dass allein die Nutzer vernetzter Geräte darüber entscheiden können, wie mit Daten umgegangen werden soll, an deren Entstehung sie mitgewirkt haben. Nutzer können dabei Unternehmen wie auch Verbraucher sein.

Quelle: www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/data-act-63748

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

AI Act „EU Artificial Intelligence Act“

(KI-Verordnung)

- AI Act ist am 1. August 2024 in Kraft getreten.
- AI Act stellt umfassende Regeln auf, um Grundrechte zu gewährleisten und Innovation zu fördern, darunter ein Verbot von Social Scoring und von bestimmten Methoden der Gesichtserkennung.
- Definition von KI, Art. 3 Nr. 1 AI Act
  - Autonomes, maschinengestütztes System
  - Anpassungsfähigkeit nach seiner Einführung
  - Verarbeitet Eingaben für explizite oder implizite Ziele
  - Generiert Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen
  - Beeinflusst physische oder virtuelle Umgebungen

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

AI Act

- Kategorisierung von KI-Systemen
  - Inakzeptables Risiko,
    z.B. zum Zweck des Social Scorings
  - Hohes Risiko,
    z.B. im Beschäftigungskontext
  - Begrenztes Risiko,
    z.B. bei Interaktion mit natürlichen Personen
  - Systemisches Risiko,
    z.B. Modelle mit allgemeinem Verwendungszweck

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

AI Act

- Anwendungsgebiete der KI
  - Bilderkennung, z.B. in der medizinischen Diagnostik
  - Spracherkennung, z.B. in Sprachassistenzsystemen
  - Semantische Spracherkennung, z.B. in Chatbots
  - Mustererkennung, z.B. Fehlermuster in der Fahrzeugelektronik
  - Prozessoptimierung

Quelle: www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz.html

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

AI Act

- Es gelten einige Übergangsfristen bis zum Inkrafttreten:
  - 6 Monate – ab dem 02.02.2025: Regelungen zu verbotenen KI-Systemen, es besteht eine umfangreiche Schulungspflicht für Mitarbeitende
  - 12 Monate – ab dem 02.08.2026: Regelungen zu KI-Modellen für allgemeine Zwecke und Sanktionen.
  - 36 Monate – ab dem 02.08.2027: Vorschriften für sog. „Integrierte KI-Systeme mit hohem Risiko“, die als Komponenten in z. B. Geräte, Fahrzeuge oder Maschinen eingebaut (Anhang I).
  - 24 Monate (Grundregel) – ab dem 02.08.2026 gelten alle übrigen Bestimmungen der KI-Verordnung.

Quelle: www.bvdnet.de

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung

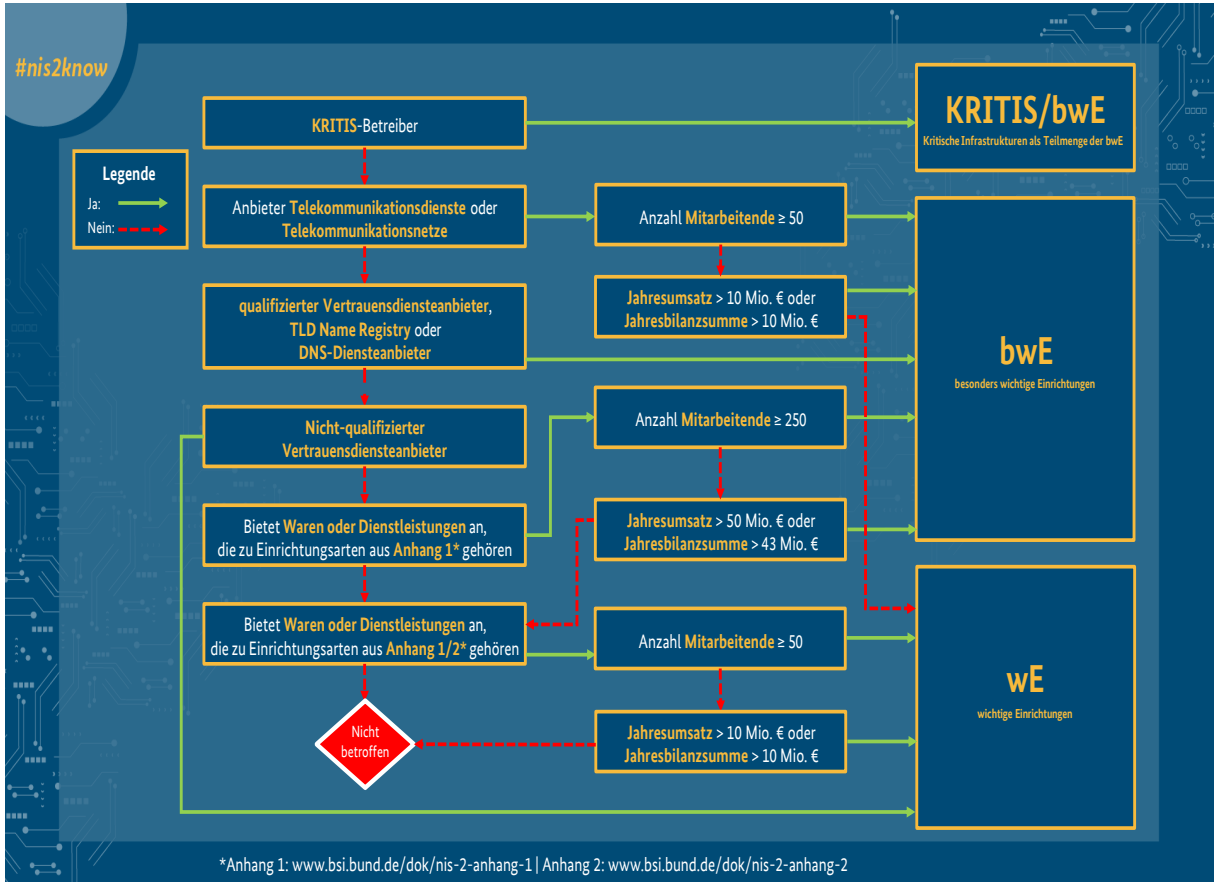
Network and Information Security Directive (NIS-2)

- Am 16. Januar 2023 ist die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) in Kraft getreten.
- Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie)
- Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen.
- Das NIS2UmsuCG (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) wurde am 24. Juli 2024 als Referentenentwurf verabschiedet. Geplant ist das Inkrafttreten im März 2025.
- Durch die Ausweitung des Anwendungsbereichs der Cybersicherheitsvorschriften auf neue Sektoren und Einrichtungen verbessert sie die Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der EU insgesamt weiter.
- Unternehmen, die von den Mitgliedstaaten als Betreiber wesentlicher Dienste in bestimmten Sektoren (wie Energie, Verkehr, Wasser, Banken, Finanzmarktinfrastrukturen, Gesundheitsversorgung und digitale Infrastruktur) eingestuft wurden, müssen geeignete Sicherheitsmaßnahmen ergreifen und die zuständigen nationalen Behörden über schwerwiegende Vorfälle informieren.
- NIS-2-Betroffenheitsprüfung des BSI (Bundesamt für Sicherheitstechnik in der Informationstechnik) verfügbar unter www.bsi.bund.de/dok/nis-2-betroffenheitspruefung

Quelle: www.bsi.bund.de/dok/nis-2

NEUE REGELUNGEN AB 2024/2025

PETER STEFFKE
Managementberatung



Entscheidungsbaum, der der NIS-2-Betroffenheitsprüfung zugrunde liegt - Quelle: www.bsi.bund.de/dok/nis-2

BERATUNG ZUM DATENSCHUTZ

PETER STEFFKE
Managementberatung

Wer darf zum Datenschutz beraten?

- ein Rechtsanwalt (Rechtsdienstleistungsgesetz)
- ein benannter Datenschutzbeauftragter (DSGVO)

NOTWENDIGKEIT UND FUNKTION EINES DATENSCHUTZ-BEAUFTRAGTEN

PETER STEFFKE
Managementberatung

Wann muss ein Datenschutzbeauftragter benannt werden?

- nach Art. 37 DSGVO
  - wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen,
  - oder die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

NOTWENDIGKEIT UND FUNKTION EINES DATENSCHUTZ-BEAUFTRAGTEN

PETER STEFFKE
Managementberatung

Wann muss ein Datenschutzbeauftragter benannt werden?

- nach §38 BDSG
  - Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
  - Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen,
  - oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

NOTWENDIGKEIT UND FUNKTION EINES DATENSCHUTZ-BEAUFTRAGTEN

PETER STEFFKE
Managementberatung

Welche Aufgaben hat ein Datenschutzbeauftragter?

- Unterrichtung und Beratung hinsichtlich Pflichten
- Überwachung der Einhaltung
- Beratung im Zusammenhang mit der DSFA
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen

NOTWENDIGKEIT UND FUNKTION EINES DATENSCHUTZ-BEAUFTRAGTEN

PETER STEFFKE
Managementberatung

Wer darf als Datenschutzbeauftragter benannt werden?

- Datenschutzbeauftragte können über die in Art. 39 DSGVO aufgezählten Aufgaben hinaus auch andere Aufgaben und Pflichten wahrnehmen (Art. 38 Abs. 6 Satz 1 DSGVO).
- Es liegt im Verantwortungsbereich des Verantwortlichen oder des Auftragsverarbeiters, dass derartige zusätzliche Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen (Art. 38 Abs. 6 Satz 2 DSGVO).
- Dies setzt voraus, dass die zu Kontrollierenden nicht selbst zu Kontrolleuren benannt werden dürfen. Das bedeutet im Einzelnen, dass Datenschutzbeauftragte zwar andere Aufgaben und Pflichten neben ihrer Tätigkeit als Datenschutzbeauftragte wahrnehmen können, diese dürfen aber nicht solche sein, welche einen engen Bezug zu Verarbeitungen von personenbezogenen Daten haben.

Quelle: www.ldi.nrw.de/datenschutzbeauftragte-faq-stellung

NOTWENDIGKEIT UND FUNKTION EINES DATENSCHUTZ-BEAUFTRAGTEN

PETER STEFFKE
Managementberatung

Wer darf als Datenschutzbeauftragter benannt werden?

Beispiele für Tätigkeitsfelder, welche zu einem Interessenkonflikt führen:

- Leitung eines Unternehmens oder einer Behörde
- Leitung der IT-Abteilung
- Leitung der Personal-Abteilung
- Beschäftigte der IT- oder Personalabteilung, wenn diese in der Lage sind, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen.

Auch die Benennung von Unternehmensinhaber*innen selbst sowie von Mitgliedern der Geschäftsleitung als Datenschutzbeauftragte ist unzulässig. Bei den Mitgliedern der Leitung von Verantwortlichen und Auftragsverarbeitern fehlt es an einer klaren Trennung zwischen den Aufgaben der Stelle und den Aufgaben der jeweiligen Datenschutzbeauftragten und somit an der notwendigen Unabhängigkeit bei der Wahrnehmung der Aufgabe als Datenschutzbeauftragte.

Quelle: www.ldi.nrw.de/datenschutzbeauftragte-faq-stellung

FOLGEN BEI DATENSCHUTZ-VERLETZUNGEN

PETER STEFFKE
Managementberatung

Was ist bei einer Datenschutzverletzung für Unternehmen (Verantwortlicher) zu tun?

- Prüfung der Meldepflicht und ggf. Meldung an die Aufsichtsbehörde (innerhalb von 72 Stunden)
- Prüfung der Informationspflicht und ggf. Information an Betroffene

FOLGEN BEI DATENSCHUTZ-VERLETZUNGEN

Welche Folgen können Datenschutzverletzungen für das Unternehmen (Verantwortlicher) haben?

- Rufschädigung
- Vertrauensverlust der Kunden
- Bußgeld
- persönliche Haftung der Geschäftsführung

EINFACHE, FLEXIBLE UND SICHERE LÖSUNG ZUM SCHUTZ VOR DATENSCHUTZ-RISIKEN

PETER STEFFKE
Managementberatung

Entscheiden Sie sich für einen externen Datenschutzbeauftragten

- Expertise
- Unabhängigkeit
- Flexibilität

KONTAKT

Peter Steffke

Managementberatung

Sanddornweg 3c

22926 Ahrensburg

04102-2178119

info@petersteffke.de

www.petersteffke.de

PETER STEFFKE
Managementberatung