JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

DigiDay

SIHK zu Hagen

Die Datenstrategie der EU

- Wie setze ich DSGVO, Data Act NIS2 & Co. effizient um?

05. Juni 2024

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Ihr Referent
Dr. Dennis Werner

- Rechtsanwalt und Notar bei der Bergfeld & Partner Rechtsanwälte Partnerschaftsgesellschaft mbB, Lüdenscheid
  - Fachanwalt für IT-Recht
  - Datenschutzbeauftragter (TÜV)
  - Mitgründer der Jurando GmbH
  - Mitautor *Heidrich/Wegener/Werner*, Datenschutz und IT-Compliance Rheinwerk Verlag

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Programm der nächsten Minuten

- Überblick über die EU-Datenstrategie
- DSGVO
- Data Act
- NIS2
- Fragen/Diskussion

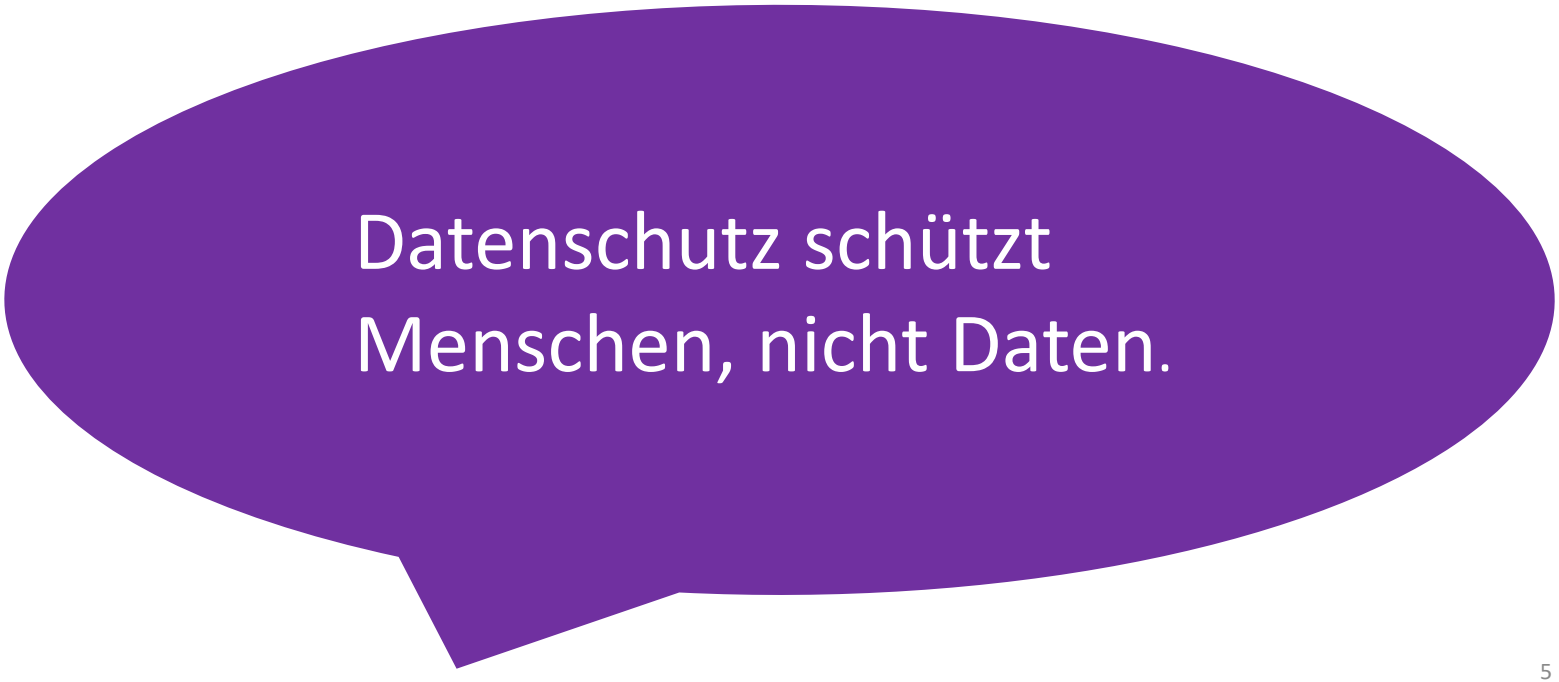
Überblick über die EU-Datenstrategie

DSGVO	(personenbezogene Daten)
DA	(faire Nutzung von Daten)
NIS2	(Cybersicherheit)
DMA	(Wettbewerb für Gatekeeper)
DSA	(Regulierung digitaler Plattformen, Dienste und Produkte)
Zukünftig:	
CRA	(Security Anforderungen für Produkte mit digitalen Elementen)

und einiges mehr …

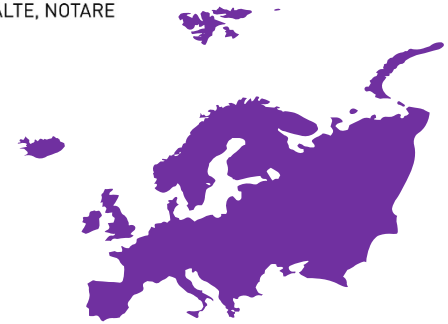
DSGVO - Ziel des Datenschutzes

Datenschutz soll vor Beeinträchtigungen des Persönlichkeitsrechts schützen:



JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE



DSGVO - Anwendungsbereich

- **Sachlicher Anwendungsbereich (Art. 2 DSGVO):**
  - Ganz od. teilweise automatisierte Verarbeitung personenbezogener Daten (pbD) sowie
  - nichtautomatisierte Verarbeitung pbD, wenn diese in einem **Dateisystem (auch geordnete Akten)** gespeichert sind oder gespeichert werden sollen.

- **Räumlicher Anwendungsbereich (Art. 3 DSGVO):**
  - Verarbeitung im Rahmen der **Tätigkeit einer Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters (unabhängig vom Ort der Verarbeitung).
  - **Angebot von Waren oder Dienstleistungen** an Personen, die sich in der EU aufhalten.
  - **Beobachtung des Verhaltens** von Personen, die sich in der EU aufhalten.

- **Wichtige Ausnahme:**
  - Verarbeitung von pbD durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (sog. **Haushaltsausnahme/Haushaltsprivileg**)

Wichtige Begriffe
(Art. 4 DSGVO)

- **Personenbezogene Daten (pbD):**

alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person (im Folgenden „betroffene Person“) beziehen;

  - Name
  - Anschrift
  - Telefonnummer
  - Personalisierte E-Mail-Adresse
  - IP-Adresse
  - Fotoaufnahmen
  - Kfz-Kennzeichen
  - Gehalt
  - Geburtsjahr

  - Dokumente/Dateien/E-Mails, in denen solche Daten vorkommen sind insgesamt pbD!

  - **Ergebnis:** Es gibt kaum Daten ohne Personenbezug

Wichtige Begriffe
(Art. 9 DSGVO)

- **Besondere Kategorien personenbezogener Daten:**
  - rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen,
  - Gewerkschaftszugehörigkeit,
  - genetischen Daten,
  - biometrischen Daten,
  - Gesundheitsdaten,
  - Daten zum Sexualleben oder der sexuellen Orientierung

  - Nicht z. B.: Bankverbindung! Die DSGVO kennt keine „sensiblen“ oder „schützenswerte“ Daten. Es gibt pbD und besondere pbD. Die Aufzählung in Art. 9 ist abschließend!

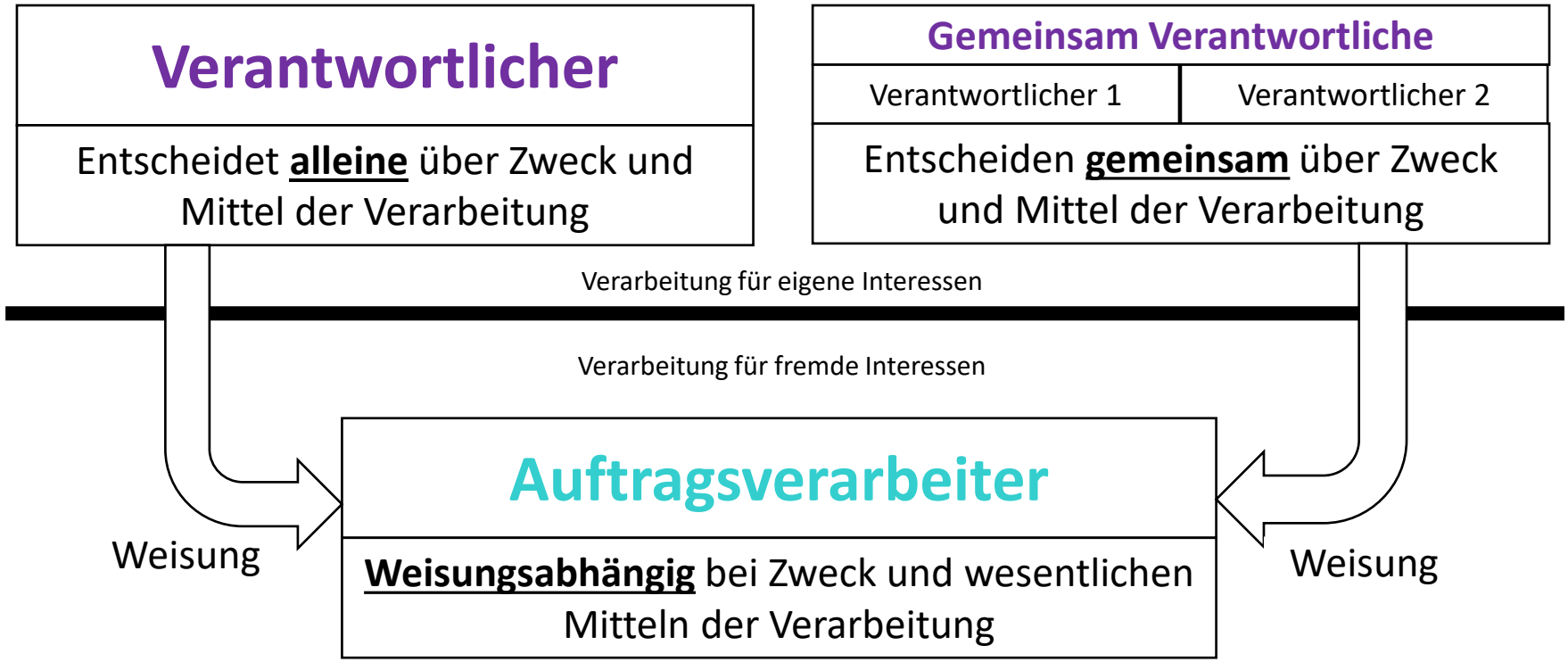
Wichtige Begriffe
(Art. 4 DSGVO)

- **Verarbeitung:**

  jeder 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;

- **Ergebnis:** Praktisch jeder Umgang mit pbD ist eine Verarbeitung iSd DSGVO.

Wichtige Begriffe (Art. 4 DSGVO)



JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Grundprinzip (Art. 6 DSGVO)

Verbot mit Erlaubnisvorbehalt

Jeder Umgang mit pbD ist verboten, wenn er nicht von einem Erlaubnistatbestand gedeckt ist.

Wichtige Erlaubnistatbestände

- **Einwilligung**
  (Art. 6 Abs. 1 lit. a DSGVO)
  - z.B.: Newsletter, Fotoaufnahmen
- **Vertragsdurchführung oder -anbahnung**
  (Art. 6 Abs. 1 lit. b DSGVO)
  - z.B. Postanschrift für Versand, E-Mail-Adresse für den Versand eines Angebots
- **Erfüllung einer rechtlichen Verpflichtung**
  (Art. 6 Abs. 1 lit. c DSGVO)
  - z.B. gesetzliche Mitteilungspflichten, Aufbewahrungsfristen nach HGB und AO
- **Berechtigtes Interesse des Verantwortlichen**
  (Art. 6 Abs. 1 lit. f DSGVO)
  - z.B. Name und Kontaktdaten eines Sachbearbeiters, Direktwerbung

Wichtige Erlaubnistatbestände

- **Besondere Erlaubnistatbestände für besondere Kategorien von personenbezogenen Daten** (Art. 9 Abs. 2 DSGVO)
- **Verarbeitungen zur Begründung, Durchführung und Beendigung von Beschäftigungsverhältnissen** (§ 26 BDSG)
- **Betriebsvereinbarungen und Tarifverträge** (Art. 88 DSGVO)
- **Konkretisierungen im BDSG und anderen nationalen Gesetzen**

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Rechenschaftspflicht

- **Art. 5 Abs. 2 DSGVO:**
  Der Verantwortliche ist für die Einhaltung der Grundsätze der Datenverarbeitung verantwortlich und muss deren Einhaltung nachweisen können („Rechenschaftspflicht“).

- **Ergebnis:** Umfassende Dokumentationspflichten und Beweislast auf Seiten des Verantwortlichen.

- Ihr Arbeitgeber muss deshalb ein **Verarbeitungsverzeichnis** führen und Technische und Organisatorische Maßnahmen (**TOM**) zum Schutz personenbezogener Daten ergreifen und dokumentieren.

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Verarbeitungsverzeichnis

- **Wer muss ein Verarbeitungsverzeichnis führen?**
  - Verantwortliche und Auftragsverarbeiter (Art. 30 DSGVO).
  - Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern greift praktisch nie.
  - Auf die Frage, ob ein Datenschutzbeauftragter benannt werden muss, kommt es nicht an.
  - Verantwortlich ist nach der DSGVO nicht mehr der DSB, sondern der Verantwortliche.

  - **Ergebnis:** Die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses besteht in praktisch jedem Unternehmen, unabhängig von der Größe und der Benennung eines DSB.

Technische und organisatorische Maßnahmen (Art. 32 DSGVO) - TOM

- Der Verantwortliche und der Auftragsverarbeiter müssen geeignete technische und organisatorische Maßnahmen für ein dem Risiko angemessenes Schutzniveau treffen.
- Abwägungskriterien:
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zweck der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere des Risikos

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

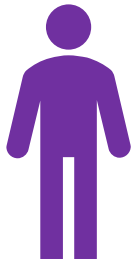
Technische und organisatorische Maßnahmen (Art. 32 DSGVO) - TOM

- Beispiele technischer Maßnahmen
  - Zutrittskontrolle (z.B. Verschließen der Türen)
  - Zugangskontrolle (z.B. Passwortschutz)
  - Zugriffskontrolle (z.B. Berechtigungskonzept)
  - Backup-Konzept
  - Malewareschutz
- Beispiele organisatorischer Maßnahmen
  - Datenschutz-Management-System
  - Verpflichtung der Mitarbeiter zur Vertraulichkeit
  - Unternehmensinterne Arbeitsanweisungen und Richtlinien zum Datenschutz
  - Regelmäßige Mitarbeiterschulungen

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Datenschutzbeauftragter (DSB)



- **Art. 37 DSGVO:**
  - Nur erforderlich, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen liegt, die umfangreiche, regelmäßige u. systematische Überwachung erforderlich machen und/oder umfangreiche Verarbeitung besonderer Arten personenbezogener Daten erfolgt.
  - Aber: nationale Regelungen beachten!
- **§ 38 BDSG:**
  - Wenn mindestens ~~10~~ **20 Mitarbeiter (Kopfzahl)** regelmäßig mit DV betraut sind
  - Wenn eine DSFA durchgeführt werden muss
  - Wenn geschäftsmäßige DV zum Zwecke der Übermittlung vorliegt
  - Wenn geschäftsmäßige DV für Zwecke der Markt- oder Meinungsforschung vorliegt

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Betroffenenrechte Systematik

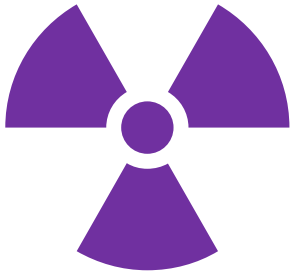
Art. 12 DSGVO

+

Art. 13/14 DSGVO	Information
Art. 15 DSGVO	Auskunft
Art. 16 DSGVO	Berichtigung
Art. 17 DSGVO	Löschung
Art. 18 DSGVO	Einschränkung der Verarbeitung
Art. 20 DSGVO	Datenübertragbarkeit
Art. 21 DSGVO	Widerspruch

=

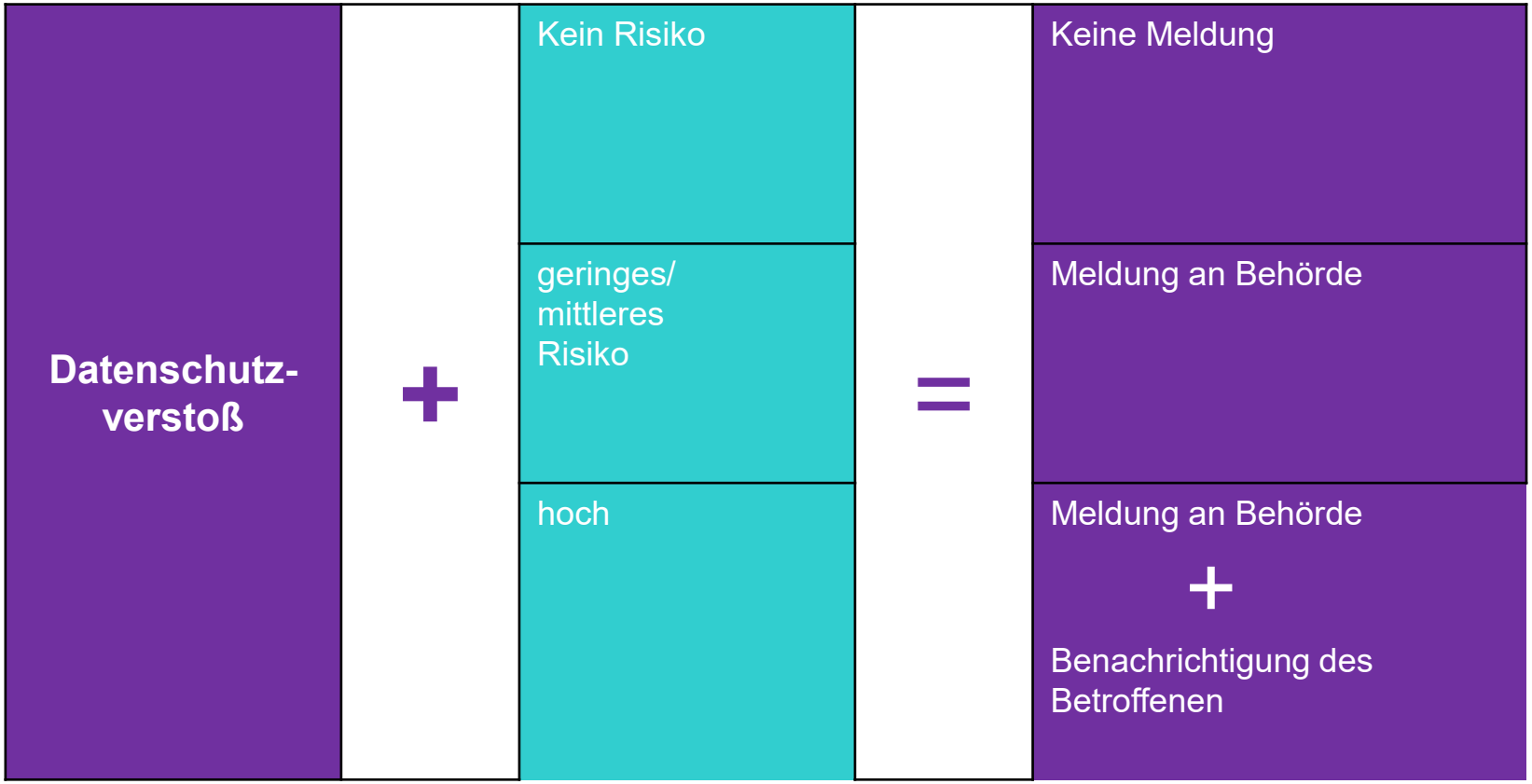
Rechtmäßiger Umgang mit Betroffenenrechten



Die Datenpanne

- Datenschutzverstoß führt grundsätzlich zur Meldepflicht, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.
- Führt sie zu einem „hohen Risiko“ muss neben der Aufsichtsbehörde auch der Betroffene informiert werden.
- Kurze Frist: 72 Stunden
- Aufsichtsbehörden stellen Meldeformulare zur Verfügung.
- Unabhängig vom Risiko ist immer eine Dokumentation anzufertigen.
- DSB einschalten!

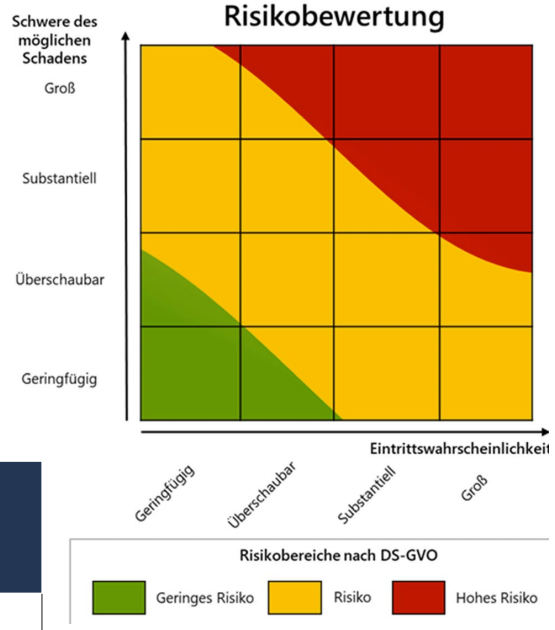
Die Datenpanne



Dokumentation von Datenpannen

Art. 33 Abs. 1 DSGVO:

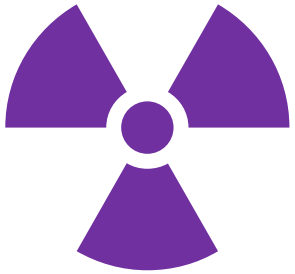
> es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. [2] Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72



Str., ob Risikobewertung zu dokumentieren ist

Risiko\Pflichten	Interne Dokumentationspflicht (Art. 33 Abs. 5 DS-GVO)	Meldepflicht an zuständige Aufsichtsbehörde (Art. 33 Abs. 1 DS-GVO)	Benachrichtigungspflicht gegenüber den betroffenen Personen (Art. 34 DS-GVO)
Voraussichtlich kein bzw. nur geringes Risiko	ja	nein	nein
Risiko	ja	ja	nein
Hohes Risiko	ja	ja	ja

LDI NRW



Die Datenpanne

- **Beispiele:**
  - Fehlversand von E-Mails/Briefen
  - Verwendung eines offenen E-Mail-Verteilers (cc:)
  - Hacker-Angriff
  - Ransomware (Verschlüsselungstrojaner)
  - Verlust eines Laptops, Smartphones oder USB-Sticks mit unverschlüsselten Daten
  - Unrechtmäßige Veröffentlichung von Daten
  - Verletzung der Vertraulichkeit durch Auskünfte an Nichtberechtigte (per Telefon oder E-Mail)
  - Falsche Zugriffsrecht von Mitarbeitern (z. B. auf Personaldaten)

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

KI-Nutzung

Handlungsempfehlungen

- Geben Sie **keine personenbezogenen Daten** (z. B. Name, Anschrift, E-Mail-Adresse) in die Eingabefelder eines KI-Systems ein.
- Laden Sie **keine Bilder** von erkennbaren real existierenden Personen an ein KI-System hoch.
- Geben Sie keine eigenen oder fremden **Geschäftsgeheimnisse** in die Eingabefelder eines KI-Systems ein.
- Prüfen Sie den von einer KI generierten Text anhand zuverlässiger dritter Quellen auf **Fehler** und **problematische Inhalte**.

DSGVO – Zusammenfassung

- Ist die Zuständigkeit für Datenschutz erklärt?
- Brauchen ich einen DSB?
- Habe ich ein VVT?
- Habe ich eine Dokumentation meiner TOM?
- Erfülle ich die Informationspflichten?
- Habe ich Prozesse zu den wichtigsten Betroffenenrechten?
- Habe ich einen Prozess zum Umgang mit Datenpannen?

Data Act (DA)

- Zeitplan: In Kraft seit 11.01.2024, Geltung weitgehend ab 12.09.2025

- Ziel: Fairer Zugang und faire Nutzung von Daten
- Daten sollen für den privaten und öffentlichen Sektor verfügbarer gemacht haben.
- Heute: Hersteller von IoT-Geräten hat faktische Datenherrschaft
- Nutzer sind aber eigentlich „Dateneigentümer“

Data Act (DA)

- Zwei große Regelungsbereiche:
  - Zugang zu Daten zum Zwecke der Förderung des Wettbewerbs rund um Daten, die mit IoT-Geräten generiert werden
  - Erleichterung des Wechsels zwischen Anbietern

Data Act (DA)

- Betroffene Daten: Personenbezogene und nicht personenbezogene Daten
- Bei IoT-Geräten alle Daten über ihre Leistung, Nutzung und Umgebung
- Bei verbunden Diensten (z. B. App) auch deren Daten (Beispiele: Fitnesstracker, dessen Daten sich vollständig nur über eine App auslesen lassen; Raumthermostat mit Cloud-Anbindung)
- Auch: virtuelle Assistenten (z. B. bei Smart-Home-Umgebungen)

Data Act (DA)

- Grundsatz: direkter Zugriff des Nutzers
- Produkt-, Dienst- und Metadaten müssen für den Nutzer einfach, unentgeltlich und in einem gängigen maschinenlesbaren Format direkt zugänglich sein (auf dem Gerät selbst oder z. B. in einer Cloud)
- Verkäufer müssen detaillierte Informationen zu Art und Umfang der Daten, der Speicherung und der Zugriffsmöglichkeiten bereitstellen
- Nutzer muss Daten auch an Dritte bereitstellen können

Data Act (DA)

- Ausnahmen vom DA:
  - Kleinstunternehmen (weniger als 10 MA und weniger als 2 Mio. Euro Jahresumsatz) und
  - Kleinunternehmen (weniger als 50 MA und weniger als 10 Mio. Euro Jahresumsatz)

Data Act (DA)

- Bereitstellung:
  - Faire, angemessene und nicht-diskriminierende Bedingungen
  - angemessene Gegenleistung

Data Act (DA)

- Anbieterwechsel:
  - Lock-In-Effekt bei Clouddiensten soll bekämpft werden
  - Wettbewerb und Innovation sollen gefördert werden
  - Kündigungsfrist darf 2 Monate nicht überschreiten und Wechsel muss innerhalb von 30 Tagen erfolgen
  - Wechselentgelte dürfen für eine Übergangszeit vereinbart werden
  - Danach bleibt die Vertragsgestaltung abzuwarten

Data Act (DA)

- Verhältnis zur DSGVO:
- Die DSGVO bleibt unberührt
- Der DA enthält keine Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten

NIS-2

- EU-Richtlinie
- Umsetzungsfrist für nationalen Gesetzgeber: 17.10.2024
- Bisher liegt nur ein Referentenentwurf vor (NIS2UmsuCG – NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)
- Schätzung: 30.000 betroffene Unternehmen (Vergleich: von NIS-1 waren ca. 2.000 KRITIS-Unternehmen betroffen)

NIS-2

- Wer ist betroffen?
  - Grundsätzlich Unternehmen ab 50 MA oder Jahresumsatz von mehr als 10 Mio. Euro bzw. Bilanzsummer mehr als 10 Mio. Euro **und**
  - Sektoren (Anhänge 1 und 2)
- Dabei Unterscheidung in „besonders wichtige“ und „wichtige“ Einrichtungen, die allerdings keine großen Auswirkungen hat.
- Wichtig: Unternehmen müssen selbst prüfen, ob sie betroffen sind.

NIS-2

- Anlage 1: Sektoren mit hoher Kritikalität (BSIG-E „Sektoren besonders wichtiger und wichtiger Einrichtungen“)
  - Energie
  - Transpost und Verkehr
  - Finanz- und Versicherungswesen
  - Gesundheit
  - Wasser
  - IT und Telekommunikation
  - Weltraum

NIS-2

- Anlage 2: sonstige kritische Sektoren (BSIG-E „Sektoren wichtiger Einrichtungen “)
  - Transpost und Verkehr
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/Herstellung von Waren (z. B. Maschinenbau, Herstellung von Kfz)
  - Anbieter digitaler Dienste
  - Forschung

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Anforderung	besonders wichtige Einrichtung		wichtige Einrichtung
	kritische Anlage	sonstige	
Registrierung und Informationsaustausch	zus. erweiterte Registrierung und Erreichbarkeit (§ 33 Abs. 2 BSIG-E)	Registrierung (§ 33 Abs. 1 BSIG-E) und Informationsaustausch (§ 6 Abs. 1 BSIG-E)	
Mindestkatalog von Maßnahmen	zus. Anforderungen (§ 31 Abs. 1 und 2 BSIG-E)	Umsetzung von Risikomanagementmaßnahmen (§ 30 Abs. 1 und 2 BSIG-E)	
Nachweis der Umsetzung	regelmäßiger Nachweis (§ 39 Abs. 1 BSIG-E)	Nachweis „auf Zuruf“ (§ 65 Abs. 3 BSIG-E)	Überprüfung „bei Verdacht“ (§ 66 BSIG-E)
Meldepflicht von Vorfällen	mehrstufiges Meldeverfahren von erheblichen Sicherheitsvorfällen (§ 32 Abs. 1 BSIG-E)		
Pflichten der Geschäftsleiter	besondere Pflichten und Haftung der Geschäftsleiter (§ 38 BSIG-E)		
zertifizierte Produkte	Verpflichtung zum Einsatz von Produkten mit Cybersicherheitszertifizierung (§ 30 Abs. 6 i. V. m. § 58 Abs. 3 BSIG-E)		
Bußgelder	bis 10 Mio. € oder 2% des Umsatzes (§ 61 Abs. 5 Nr. 2 lit a und Abs. 6 BSIG-E)		bis 7 Mio. € oder 1.4 % des Umsatzes (§ 61 Abs. 5 Nr. 2 lit 2 und Abs. 7 BSIG-E)

NIS-2-Richtlinie (EU) 2022/2555 und NIS2UmsCG-E (Stand: 7. Mai 2024)

Link zum Blogbeitrag: https://we.secure-your.it/2024/05/08/schaubild-zumnis2umscg-e/

NIS-2

- Wer ist betroffen?
  - Auch untergeordnete und reine Nebentätigkeiten reichen (Beispiele: PV-Anlagen zum Eigenverbrauch als Erzeuger im Energiesektor)
  - Konzern-IT, die bei einer Tochtergesellschaft zentralisiert ist, kann ein Rechenzentrumsdienst sein
  - Achtung: Lieferketten! (z. B. Produktion für Automobilhersteller)
  - Registrierungspflicht innerhalb von 3 Monaten

NIS-2

- Risikomanagementmaßnahmen:
  - Risikoabschätzung
  - geeignete und verhältnismäßige TOM unter Berücksichtigung des Standes der Technik
  - nicht: in jedem Fall absolute Sicherheit oder höchstmöglichstes Sicherheitsniveau

NIS-2

- Risikomanagementmaßnahmen:
  - Mindestmaßnahmen (Auszug aus § 30 BSIG-E): Backup-Management, Cybersicherheitsschulungen, Zugangskontrollkonzepte, ggf. Verschlüsselung
  - Achtung! Sicherheit der Lieferkette! Anpassung der vertraglichen Vereinbarungen (z. B. auch Kontrollbefugnisse, Verpflichtungen zu Sicherheitsupdates etc.)

NIS-2

- Informationspflichten:
  - Meldepflichten (i.d.R. ggü. dem BSI als Aufsichtsbehörde), Frühmeldung nach 24 Stunden, 72 Stunden Aktualisierung mit Bewertung, 1 Monat detaillierte Beschreibung
  - Achtung! NIS-2-Aufsichtsbehörde muss u. U. DSGVO-Aufsichtsbehörde informieren. Denken Sie an die ggf. erforderliche Meldung einer Datenpanne.
    - Praxistipp: Zentrale Stelle im Unternehmern zur Koordination der Meldungen etablieren

NIS-2

- Sanktionen:
  - Bußgelder bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes
  - Leitungspersonen (Geschäftsführer/Vorstand) kann persönlich verantwortlich gemacht werden
  - Leitungspersonen müssen die Risikomanagementmaßnahmen ausdrücklich genehmigen und die Umsetzung überwachen. NIS2 ist Chefsache!
  - Leitungspersonen müssen an Schulungen teilnehmen und Kenntnisse zur Identifizierung und Bewertung von Risiken und Risikomanagementmaßnahmen erwerben
  - „Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter“

NIS-2

- Sanktionen:
  - Unternehmen dürfen nicht auf Ersatzansprüche gegen Leitungspersonen verzichten!
  - Bußgeldregress möglich!
  - Aufsichtsbehörden können Leitungspersonen als ultima ratio von ihren Aufgaben entbinden!

NIS-2

- Praxistipp:

- Prüfen Sie schon jetzt, ob Sie potenziell von NIS-2 betroffen sind
  - Sprechen Sie uns gerne an ☺

- Halten Sie die Entwicklung des Umsetzungsgesetzes im Auge

JURANDO

BERGFELD&PARTNER
RECHTSANWÄLTE, NOTARE

Vielen Dank
für Ihre Aufmerksamkeit!

Gibt es Fragen? Diskussionen?

Kontakt:

- Dr. Dennis Werner
- d.werner@bergfeldonline.de