Datenschutz für (Chaos-)Vereine in der Praxis

rhandos(sie/ihr)
GPN24

rhandos
(sie/ihr)

Macht Ding mit Verwaltungsrecht

Datenschutzbeauftragte CCCHH

Was sind meine Pflichten?

Hilfe, wo fange ich an?

Get yourself a DSB ♥

Das ist kein Rechtsgrundlagen-Talk!

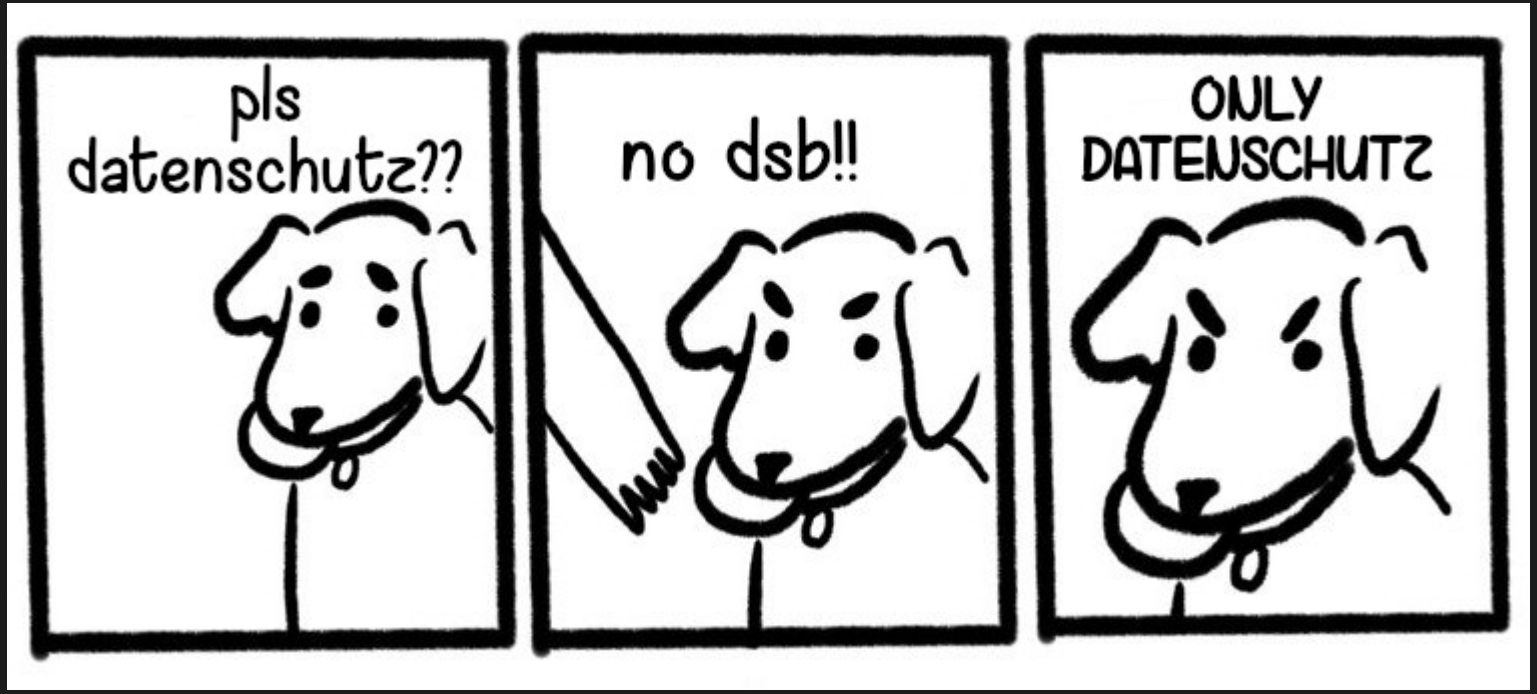
(also nur so zu ~75%)

Datenschutz im Verein

Michael Stemann

Datenschutzrechte für Betroffene

rhandos


pls
datenschutz??
no dsb!!
ONLY
DATENSCHUTZ

Art. 37 DSGVO - Benennung einer Datenschutzbeauftragten

- Behörde oder öffentliche Stelle

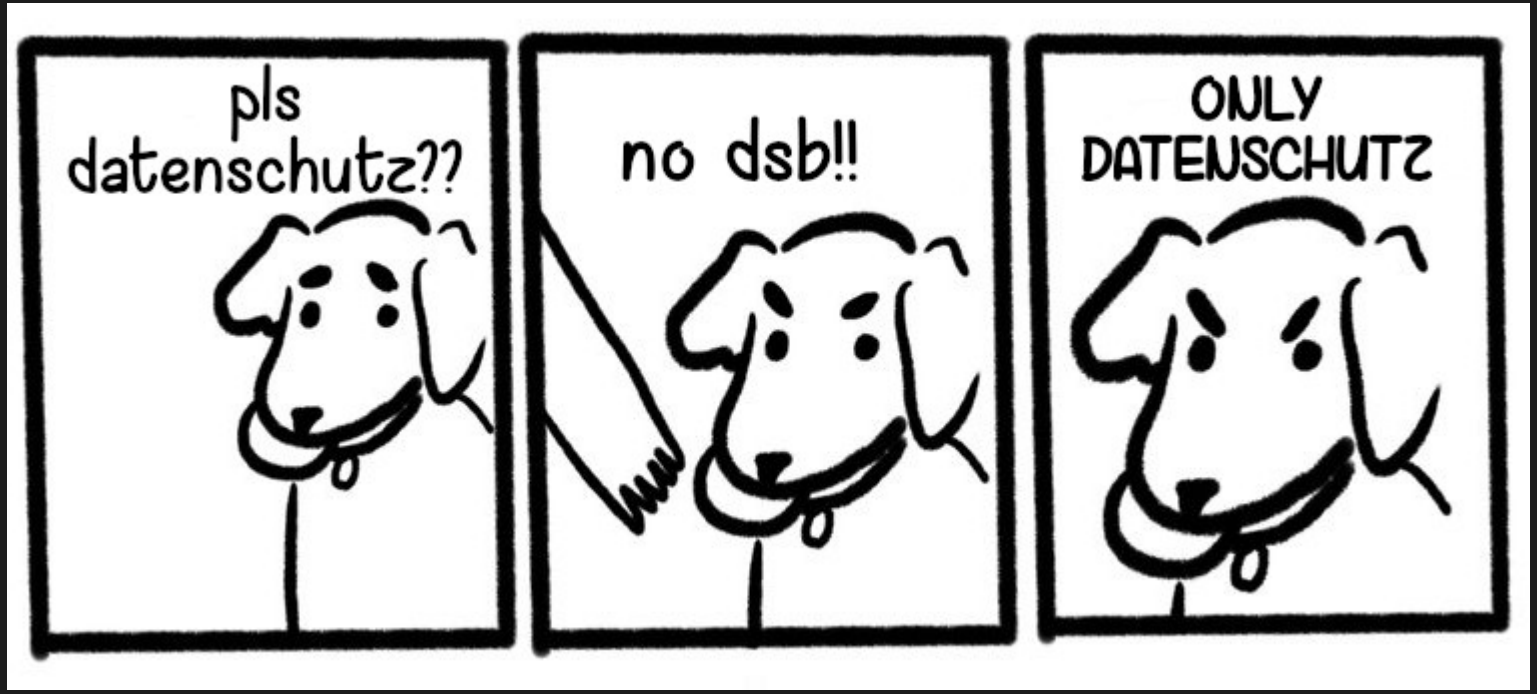
- umfangreiche regelmäßige und systematische Überwachung

- umfangreiche Verarbeitung besonderer Kategorien von Daten oder über strafrechtliche Verurteilungen und Straftaten ?

§ 38 BDSG - Datenschutz-beauftragte nichtöffentlicher Stellen

- in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt !

“Der Bund wird bis zum 31.12.2026 eine Aufhebung des § 38 Abs. 1 BDSG einbringen und damit die Pflicht zur Bestellung von Datenschutzbeauftragten im nichtöffentlichen Bereich auf die Regelung in Art. 37 DSGVO beschränken.”


pls
datenschutz??
no dsb!!
ONLY
DATENSCHUTZ

DSB-Aufgaben

- Unterrichtung und Beratung der Verantwortlichen
- Überwachung der Einhaltung der DS-Vorschriften
- Beratung zu DSFA (auf Anfrage)
- Zusammenarbeit mit und Anlaufstelle für Aufsichtsbehörde

DSB berät

Verantwortliche ist verantwortlich

Was sind meine Pflichten als Verantwortliche?

1) DSGVO-Grundsätze einhalten (Art. 5 ff. DSGVO)

2) Verarbeitungsverzeichnis (Art. 30 DSGVO)

3) Datenschutzinfos (Art. 13/14 DSGVO)

4) AV/gem. Verarbeitung (Art. 26, 28 DSGVO)

5) Betroffenenrechte (Art. 12 ff. DSGVO)

6) Konzept für Datenpannen (Art. 33 f. DSGVO)

(nicht abschließend)

Verarbeitungsgrundsätze (Art. 5 DSGVO)

1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

2) Zweckbindung

3) Datenminimierung

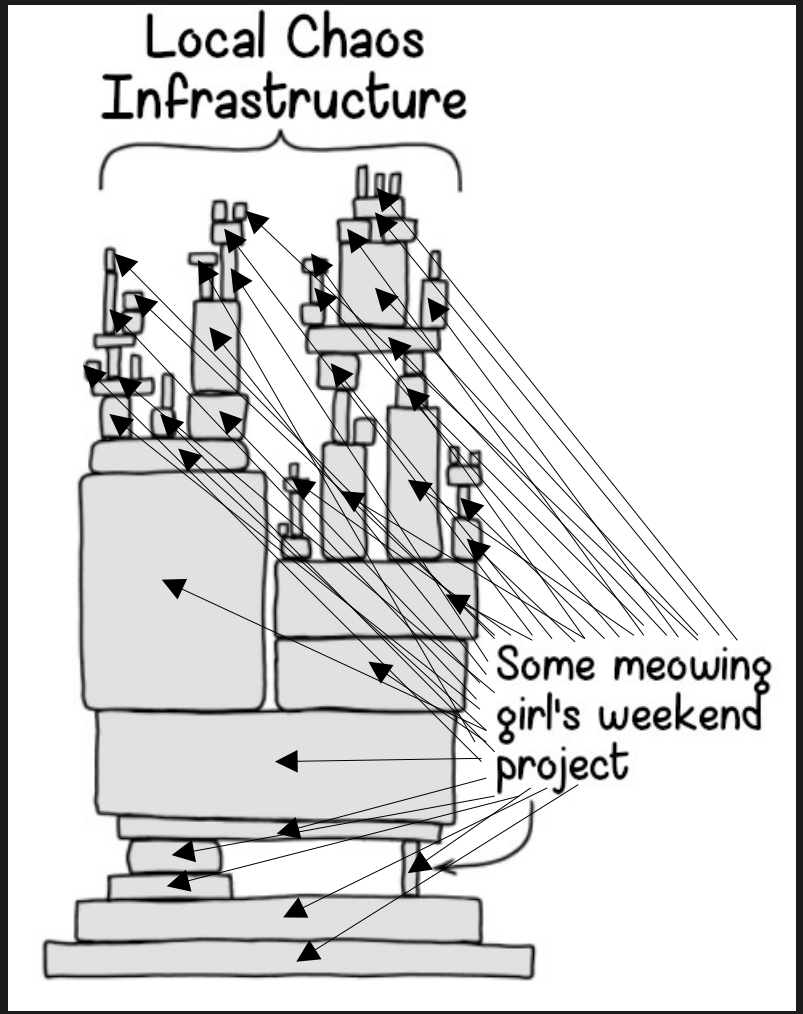
4) Richtigkeit

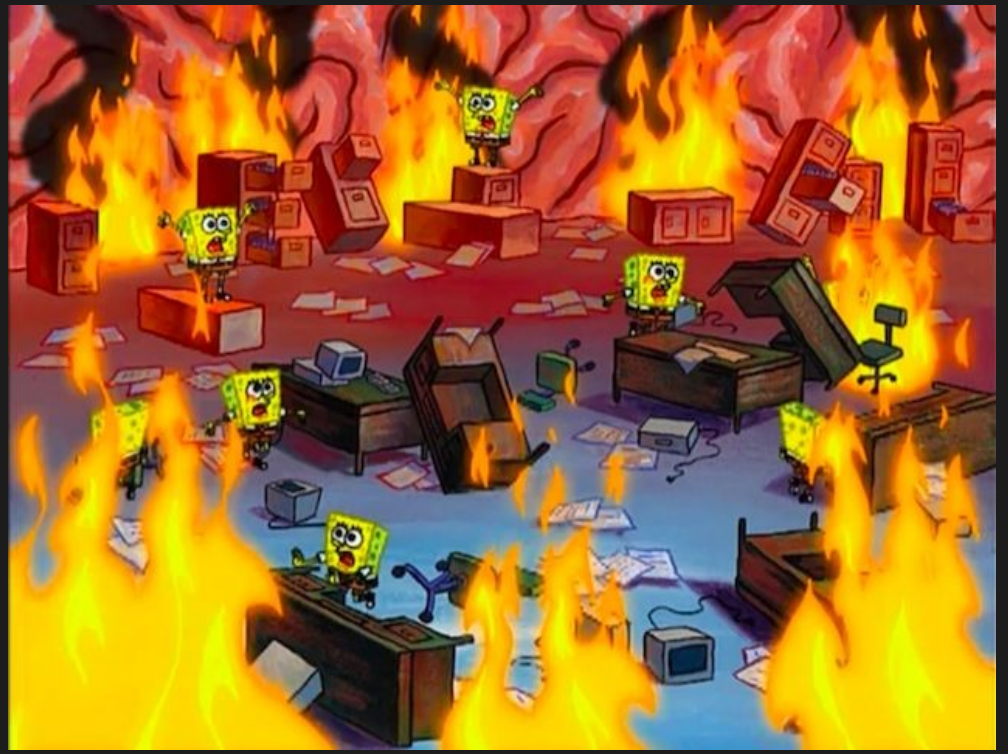
5) Speicherbegrenzung

6) Integrität und Vertraulichkeit

7) Rechenschaftspflicht

Wie setze ich das alles um?!


Local Chaos
Infrastructure
Some meowing
girl's weekend
project



1) Prozesse dokumentieren

(Art. 30 DSGVO)

Schritt 1: Prozesse bestimmen

Was verarbeitet personenbezogene Daten?

Für welche Prozesse bin ich verantwortlich?

Schritt 2: Prozesse ordnen

Kernprozesse bestimmen, priorisieren

Extern: Website, Nextcloud, Git...

Intern: Mitgliederverwaltung, Kasse, …

Orgatipp, keine gesetzliche Definition!

Gefundene Prozesse in Verarbeitungsverzeichnis überführen

Prozessverantwortliche bestimmen (jemensch™ macht das)

Verzeichnis zusammen mit Prozessverantwortlicher ausfüllen

- Name & Kontakt Verantwortliche
- Zwecke der Verarbeitung
- Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien von Empfängern
- ggf. Übermittlungen an Drittland oder int. Organisation
- Löschfristen
- Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 Abs.1 DSGVO

Beispielprozess (1)

Verantwortliche	CCC Medientheater e.V.
Prozess	Mitgliederverwaltung
Zwecke	Verwaltung der Mitglieder, Mitgliedsstatus, Beitragszahlung

Beispielprozess (2)

Kategorien betroffener Personen	Mitglieder
Kategorien betroffener Daten	Name, Anschrift, E-Mail, Ein-/Austrittsdatum, Förder-/Vollmitglied
Kategorien von Empfängern	Keine

Beispielprozess (3)

Drittlandstransfer	Nein
Löschfristen	3 Jahre nach Austritt zum Jahresende
TOMS	Siehe IT- und Sicherheitskonzept

+ Anlage 1: ITSM-Konzept 

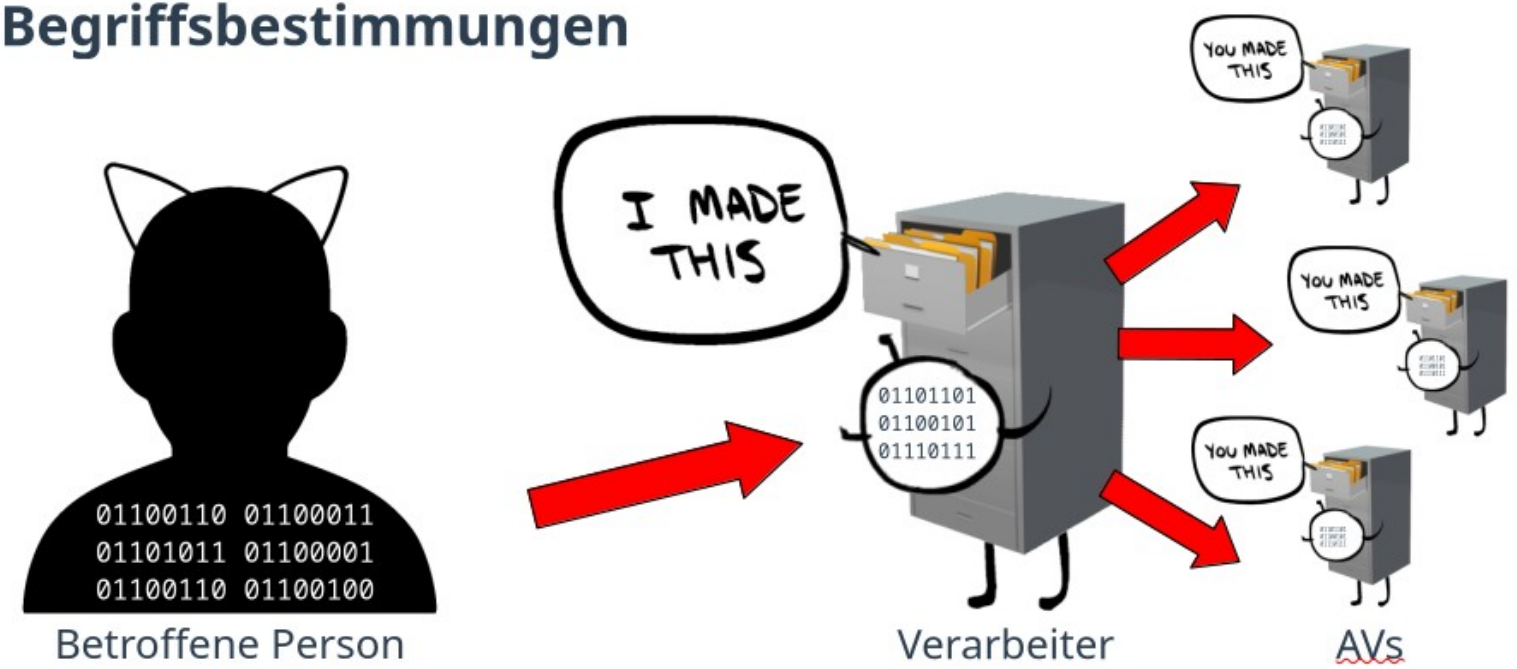
Beispielprozess (3)

Sinnvolle weitere Felder:

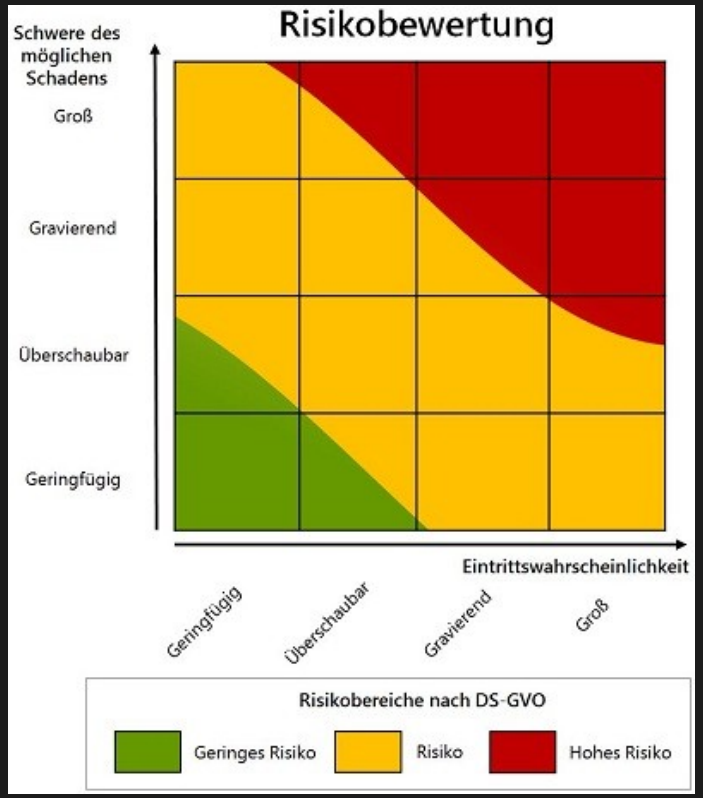
- Prozessverantwortliche (intern)
- Rechtsgrundlage (Art. 6 DSGVO)
- Prozess erstellt/geändert/Version
- Verknüpfte AVVs (schließt AVVs ab!)
- Schwellwertanalyse / DSFA

Exkurs: Auftragsverarbeitung

- **Begriffsbestimmungen**



Exkurs: Schwellwertanalyse/DSFA



2) Prozesse anpassen

Verarbeitung ohne RGL

- Random Mailingliste ohne Einwilligung
- Alle Mitglieder haben automatisch Nextcloud-Account

Verarbeitung ohne RGL

- RGL finden
- Einwilligung einholen (oft aufwändig)
- oder: Verarbeitung schnell beenden

Verstoß gegen DS-Grundsätze

- z.B. Datenminimierung, AV ohne AVV
- Nicht erforderliche Daten verarbeitet (Geburtsdatum, Anrede, Telefonnummer, …)
- Adressbuch exposed alle Mitglieder untereinander

3) Datenschutzinformationen

(Art. 13 & 14 DSGVO)


THIS IS WHERE I PUT
MY DATENSCHUTZERKLÄRUNG
IF I HAD ONE

Kategorien betroffener Personen

Da wir keine Daten erheben, gibt es auch keine betroffenen Personen.

Grundlage: Verarbeitungsverzeichnis :)

- Name & Kontakt Verantwortliche
- *ggf. Kontakt DSB*
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorien von Empfängern
- *ggf. Übermittlungen an Drittland oder int. Organisation*
- Speicherdauer
- *ggf. Verpflichtung und Nachteile bei Nichtverarbeitung*
- *ggf. Bestehen automatisierte Entscheidungsfindung*
- Belehrung über Betroffenenrechte

- Name & Kontakt Verantwortliche
- *ggf. Kontakt DSB*
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorien von Empfängern
- *ggf. Übermittlungen an Drittland oder int. Organisation*
- Speicherdauer
- *ggf. Verpflichtung und Nachteile bei Nichtverarbeitung*
- *ggf. Bestehen automatisierte Entscheidungsfindung*
- Belehrung über Betroffenenrechte

3.2.4 Rechtsgrundlage

Rechtsgrundlage für den technisch erforderlichen Betrieb ist Art. 6 Abs. 1 S. 1 lit. f DSGVO (berechtigtes Interesse an Betrieb und Sicherheit der Keycloak-Instanz).

Rechtsgrundlage für die Nutzung eines CCCHH-ID-Accounts und die Weitergabe deiner Nutzerdaten in Drittsysteme über den Single-Sign-On ist deine Einwilligung, Art. 6 Abs. 1 S. 1 lit. a DSGVO.

Erteilst du deine Einwilligung nicht, kannst du ggf. Dienste, die die CCCHH-ID verwenden, nicht verwenden, wenn für bestimmte Funktionen ein Account erforderlich ist.

5. Betroffenenrechte

Du hast gegenüber uns folgende Rechte hinsichtlich der dich betreffenden personenbezogenen Daten:

- Recht auf Auskunft
- Recht auf Berichtigung oder Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Widerspruch gegen die Verarbeitung
- Recht auf Widerruf der Einwilligung

6. Recht auf Beschwerde bei der Aufsichtsbehörde

Du hast das Recht, bei einer Aufsichtsbehörde Beschwerde einzulegen, wenn du der Meinung bist, dass unsere Verarbeitung deiner personenbezogenen Daten gegen die gültigen Datenschutzgesetze verstößt.

Form und Zeitpunkt

- Zum Zeitpunkt der Erhebung
- präzise, transparente, verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache
- Medienbruch ok!

Exkurs: § 25 TDDDG

- Einwilligung für lokal gespeicherte Informationen erforderlich
- Betrifft z.B. Cookies, Local Storage
- Wichtige Ausnahme: Keine Einwilligung bei technisch erforderlichen Informationen (z.B. Session Cookies)
- Für technisch nicht erforderliche: Consent Management

1) DSGVO-Grundsätze einhalten (Art. 5 ff. DSGVO) ✅

2) Verarbeitungsverzeichnis (Art. 30 DSGVO) ✅

3) Datenschutzinfos (Art. 13/14 DSGVO) ✅

4) AV/gem. Verarbeitung (Art. 26, 28 DSGVO) ✅

5) Betroffenenrechte (Art. 12 ff. DSGVO)

6) Konzept für Datenpannen (Art. 33 f. DSGVO)

4) Management von Betroffenenanfragen

Übliche Anfragen:

- Auskunft, Art. 15 DSGVO
- Berichtigung, Art. 16 DSGVO
- Löschung, Art. 17 DSGVO
- Widerruf / Widerspruch, Art. 7 (3), 21 DSGVO

→ **Siehe Betroffenenrechte-Talk**

Grundsätze:

- Unentgeltlich
- Unverzüglich, spätestens binnen eines Monats
- (Ausnahmen bei besonders komplexen Anträgen möglich)

- Wer beantwortet Gesuche?
- Wer überwacht den Eingang und die Fristen?
- Eingangsbestätigung!

5) Management für Datenschutzvorfälle

Liegt eine Datenpanne vor?

Art. 33 Abs. 1 S. 1 DSGVO:
“Verletzung des Schutzes personenbezogener Daten”

- Vernichtung
- Verlust
- Veränderung
- unbefugte Offenlegung/unbefugter Zugriff

Datenpanne? Meldung!

- An Aufsichtsbehörde
- Binnen 72 Stunden ab Bekanntwerden (!)
- Entfällt nur bei geringem Risiko für Rechte und Pflichten betroffener Personen
- Im Zweifel: Verdachtsmeldung!

Der Landesbeauftragte für den Datenschutz Niedersachsen

Niedersachsen. Klar.

Startseite

Hinweis: Bitte beachten Sie, dass die Abgabe einer Meldung nach Art. 33 DSGVO bei einem geringen Risiko im Sinne des Kurzpapiers Nr. 18 der Datenschutzkonferenz nicht erforderlich ist (siehe unten Ziffer 7.4).

Benachrichtigung (* = Pflichtangaben)

Art der Meldung *

- (●) Vollständige Neumeldung
- ( ) Vorläufige Neumeldung (es erfolgt noch eine spätere ergänzende Meldung)
- ( ) Ergänzende Meldung

1. Über den Meldenden

1.1 Kontaktdaten des Verantwortlichen (* = Pflichtangaben)

Name Ihrer Organisation (z.B. Firma) *	Name
Vertreten durch (z. B. Geschäftsführer, Vorstand)	Funktion, Name
Straße und Hausnummer *	Straße und Hausnummer der Organisation
PLZ und Ort *	Postleitzahl und Ort der Organisation
Registerangaben: Registernummer (z.B. Handelsregister), Angabe des Gerichts	Ihre Registernummer, Ihr Registergericht
Umsatzsteuer-ID	Ihre Umsatzsteuer-ID
Internetseite	Internetseite der Organisation
E-Mail-Adresse *	E-Mail-Adresse
Telefonnummer	Telefonnummer

Datenpanne? Benachrichtigung!

- An betroffene Person(en)
- Bei voraussichtlich hohem Risiko für Rechte und Pflichten betroffener Personen

Wann melde ich was?

Risiko	Meldung Aufsichtsbehörde	Meldung betroffene Personen
gering	*nein*	*nein*
mittel	**ja**	*nein*
hoch	**ja**	**ja**

1) DSGVO-Grundsätze einhalten (Art. 5 ff. DSGVO) ✅

2) Verarbeitungsverzeichnis (Art. 30 DSGVO) ✅

3) Datenschutzinfos (Art. 13/14 DSGVO) ✅

4) AV/gem. Verarbeitung (Art. 26, 28 DSGVO) ✅

5) Betroffenenrechte (Art. 12 ff. DSGVO) ✅

6) Konzept für Datenpannen (Art. 33 f. DSGVO) ✅

Erfindet das Rad nicht neu!

Muster und Hilfen verwenden

z.B. Muster-Verarbeitungsverzeichnis

z.B. Kurzpapiere der DSK

Austausch im Chaos!

Angebot: Matrix-Gruppe ”Chaos macht Datenschutz”

matrix #datenschutzaustausch:hamburg.ccc.de