Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Datenpannen
- Eine Panne kommt selten allein -

LfDI Dr. Stefan Brink

6. Dezember 2018
Wiesbaden

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

I. Zweck und Bedeutung

⇒**Transparenz** → Betroffener soll rechtzeitig und angemessen reagieren können

⇒**Präventive Wirkung** (Anreiz für Maßnahmen zur Verhinderung meldepflichtiger Ereignisse)

⇒**Schlüsse** auf **zukünftige Gefahren** möglich

I. Zweck und Bedeutung

⇒**Vermeidung + Minimierung** von **Folgeschäden, <u>EWG 85</u>**:

*„**physischen, materiellen oder immateriellen Schaden** für natürliche Personen nach sich ziehen, wie etwa **Verlust der Kontrolle** über ihre personenbezogenen Daten oder **Einschränkung ihrer Rechte, Diskriminierung, Identitäts-diebstahl oder -betrug, finanzielle Verluste, unbefugte Auf-hebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit** von dem Berufsgeheimnis unterliegenden Daten oder andere **erhebliche wirtschaftliche oder gesellschaftliche Nachteile**“*

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

II. Datenpannen nach BDSG: § 42a

Best of:

- numerus clausus der meldepflichtigen Daten (Risikodaten):

  => besondere Arten pbD (§ 3 Abs. 9)
  => Berufsgeheimnisdaten
  => pbD zu Bank- und Kreditkartenkonten

  Fazit: bis zu <u>75 % der Meldungen ohne rechtl. Anlass</u>

- Voraussetzung: schwerwiegende Beeinträchtigungen drohen

Fazit: weitere 50 % der Meldungen ohne Pflicht

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Datenpannen nach BDSG: § 42a

Best of:

- nachgelagerte Meldepflicht Betr. (erst begrenzen, dann mitteilen; Schutz der Strafverfolgung)
- Veröffentlichung anstatt unverh. Mitteilung (ND/junge welt [fdj])
- Verwertungsverbot: nemo tenetur (§ 42a Satz 6)

  Fragen: - nur für pflichtige Meldungen?
  - auch bei Vorsatztaten?

- Meldepflichtige: verantwortliche Stelle (+)
  ADV (-)
- § 43 Abs. 2 Nr. 7 BDSG

III. Die EU-Datenschutz-Grundverordnung

Art. 33 Meldepflicht

- risikobasierter Ansatz:

  - Wegfall der Meldepflicht bei negativer Risikoprognose

  - Prognoserisiko des Verantwortlichen

  - Dokumentationspflicht gegenüber AB (Abs. 5)

  => doppelt begrenzte Risikobasierung (≠ DV / AB!)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Die EU-Datenschutz-Grundverordnung

Art. 33 Meldepflicht

- Auch für A(D)V

- Inhalte der Meldepflicht (Abs. 3)
  - ungefähre Anzahl der Betroffenen
  - Angabe bDSB

- Pflicht zur Vorabmeldung von Teil-Informationen

- Dokumentation-, keine Informationspflicht

- **kein Verwertungsverbot!**

Die EU-Datenschutz-Grundverordnung

- Art. 33: Meldung an die AB /
  Art. 34 Benachrichtigung des Betroffenen

Art. 34 Benachrichtigungspflicht

- risikobasierter Ansatz II:

  - Pflicht des Verantwortlichen nur bei pos. Risikoprognose

  => echte Risikobasierung

- Pflicht nur des Verantwortlichen, **≠ A(D)V**

Die EU-Datenschutz-Grundverordnung

Art. 34 Benachrichtigungspflicht

- begrenzte Informationspflicht:

  - klare und einfache Sprache

- Wegfall der Pflicht (Abs. 3)

  - wirksame Verschlüsselung (a)
  - Risikominimierung (b)
  - Veröffentlichung anstatt unverh. Mitteilung (c)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Die EU-Datenschutz-Grundverordnung

Art. 34 Benachrichtigungspflicht

- Rolle der AB:

  => AnO der nachgeholten Benachrichtigung

  => Feststellung der Vss. Abs. 3 (Wegfall Benachrichtigung)

- **kein Verwertungsverbot!**

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

IV. Voraussetzungen der Meldepflicht

Verletzung des Schutzes personenbezogener Daten:

- (P) Was sind genau pbD? (obj. oder subj. Personenbezug? Rückführbarkeit anonymisierter Daten?)
- Art. 29 WP: **Verlust von CD mit verschlüsselten Daten ist meldepflichtig!!**
- (P) Vorübergehende Unterbrechung der Datenverfügbarkeit? (Aktuelle Diskussion d. Art. 29 WP)

IV. Voraussetzungen der Meldepflicht

Verletzung des Schutzes personenbezogener Daten:

- ***"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted or otherwise processed"***

IV. Voraussetzungen der Meldepflicht

- destruction: Daten existieren nicht mehr
- damage: Änderung, Beschädigung, Unvollständigkeit
- loss of pD: Kontroll- oder Zugangsverlust
- unauthorised/unlawful processing: Unauthorisierte/rechtswidrig Eröffnung/Zugang von/zu Daten

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

V. Form und Inhalt

Inhaltliche Mindestanforderungen in Art. 33 Abs. 3 DS-GVO:

- Art der Verletzung, Kategorien betroffener Pers. + Kategorien und Anzahl betroffener Datensätze
- Name + Kontakt von DSB oder Anlaufstelle
- Beschreibung wahrscheinlicher Folgen
- Beschreibung von Maßnahmen zur Behebung oder Abmilderung
- Falls nicht gleichzeitig verfügbar: Schrittweise zur Weitergabe der Information, Art. 33 Abs. 4 DS-GVO

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

V. Form und Inhalt

Data breach notification form

Art 33 of the General Data Protection Regulation obligates data controller to notify data breach to the relevant Supervisory Authority

Field name	management rules	Type of field	Values (if applicable)	Initial State	size of field	Data format expecte
0. Data breach notification						
Type of notification		radio button	complete notification, preliminary notification, complementary/amended notification	unselected	n/a	list of value
ID of previously notified breach	visible only If type of notification = complementary/amended notification. Check existence of a previously notified data breach	free text	n/a	empty	size of breach ID	text
date of previous notification	visible only If type of notification = complementary/amended notification. Check existence of a previously notified data breach	date	n/a	empty	n/a	time/day/month/yea
1. About you						
1.1 Contact details						
Organisation officially registered number	If available check chamber of commerce for retrieval of the identification of the organisation	free text	n/a	empty	n/a	text
VAT Number	check consistency of the number with the Commission website : http://ec.europa.eu/taxation_customs/vies/technicalInformation.html	free text	n/a	empty	15 caracters	text
Organisation number	Check existence of an organisation with this number	free text	n/a	empty	n/a	text
Name of the organisation		free text	n/a	empty	n/a	text
Address and any relevant contact details of the Organisation		free text	n/a	empty	n/a	text
Name and function of the reporting person		free text	n/a	empty	n/a	text
Reporting person's contact details		free text	n/a	empty	n/a	text
Name and function of the person who can		free text	n/a	empty		text

VI. Zeitpunkt der Meldung

- **Unverzüglich** und **möglichst binnen 72 Stunden**, Art. 33 Abs. 1 S. 1 DS-GVO
- Bei späterer Meldung an AB **Begründung** notwendig, Art. 33 Abs. 1 S. 2 DS-GVO
- Keine Vorgaben der DS-GVO an Begründung bezgl. Umfang oder Inhalt (Leitlinien der AB für die Praxis möglich)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

VII. Dokumentation

- Dokumentationspflicht = Konkretisierung der allg. Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO
- Dokumentation von **Verletzungen** des Schutzes personenbezogener Daten, der **Auswirkungen** und der **ergriffenen Abhilfemaßnahmen, Art. 33 Abs. 5 DS-GVO**
- Zusätzlich: Alle damit in Zusammenhang stehenden Daten und Fakten

=> Umfang der Dokumentationspflicht weiter als Inhalt der Meldepflicht aus Art. 33 Abs. 3 DS-GVO

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

VIII. Sanktionen von Verstößen gegen die Meldepflicht nach Art. 33 DS-GVO

Art. 83 Abs. 1 DS-GVO:

→ „*wirksam, verhältnismäßig und abschreckend*“

Art. 83 Abs. 4 lit. a DS-GVO:

- Verstoß gg. **Meldepflicht** (Art. 33 Abs. 1 DS-GVO) oder **Dokumentationspflicht** (Art. 33 Abs. 5 DS-GVO)
- **Geldbuße** von bis zu **10.000.000 €** oder im Fall eines Unternehmens **2 % des gesamten weltweit erzielten Jahresumsatzes**

IX. Kein Verwertungsverbot

<u>EWG 87:</u>

„Die entsprechende Meldung **kann** zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.“

IX. Kein Verwertungsverbot?

(P) § 43 Abs. 4 BDSG n.F.:

„Eine Meldung, die der Meldepflichtige nach Artikel 33 der Verordnung (EU) 2016/679 erteilt hat oder eine nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 erfolgte Benachrichtigung darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder in § 52 Absatz 1 der Strafprozessordnung bezeichnete Angehörige des Meldepflichtigen oder Benachrichtigenden **nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden**."

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Datenschutz heute

[1)] … der **unabhängigen** Datenschutzaufsichtsbehörden

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Rolle der Aufsichtsbehörden

Online-Beschwerdeformular	Meldung Datenpannen	Meldung DSBs
März: 41		
April: 61		
Mai: 160	Mai: 25	Mai: 14.288
Juni: 170	Juni: 94	Juni: 3.221
Juli: 168	Juli: 105	Juli: 1.743

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vielen Dank!