Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Bayerisches Landesamt für Datenschutzaufsicht

Datenpannen

Sicht der Aufsichtsbehörde: Wann & wie ist zu melden? Umgang mit den Datenpannenmeldungen

Dr. Stefan Brink
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

+

Thomas Kranig
Bayer. Landesamt für Datenschutzaufsicht

Agenda

1. Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?
2. Meldeverhalten in Deutschland und Europa
3. Wie geht die Aufsicht mit den Meldungen um?
4. Art. 33 DS-GVO und Geldbuße – geht das?
5. Ausblick

Agenda

1. **Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?**
2. Meldeverhalten in Deutschland und Europa
3. Wie geht die Aufsicht mit den Meldungen um?
4. Art. 33 DS-GVO und Geldbuße – geht das?
5. Ausblick

Grundsätze der Verarbeitung pbD
Art. 5 Abs. 1

1 **Verantwortlicher muss rechtmäßigen Datenumgang nachweisen (Rechenschaftspflicht, Art. 5 Abs. 2)**

2 **Verantwortung des Verantwortlichen**
Art. 24

DV by design & by default Art. 25	**Gemeinsam Verantwortliche** Art. 26	**Auftrags-verarbeiter** Art. 28
Verzeichnis Art. 30	**Sicherheit der Verarbeitung** Art. 32	**Meldung von Verletzungen** Art. 33, 34
DS-Folgen-abschätzung Art. 35, 36	**Datenschutz-beauftragter** Art. 37 - 39	**Übermittlung Drittländer** Art. 44 - 49

Rechte der betroffenen Person
Art. 12 - 23

3 **Transparente Information, Kommunikation und Modalitäten**
Art. 12

Erhebung Art. 13, 14	**Auskunft** Art. 15	**Widerspruch** Art. 21
	Berichtigung Löschung Einschränkung Art. 16 - 19	**Automatisierte Entscheidung** Art. 22
	Datenüber-tragbarkeit Art. 20	**Benachrichtigung von Verletzung** Art. 34

Information

Kommunikation

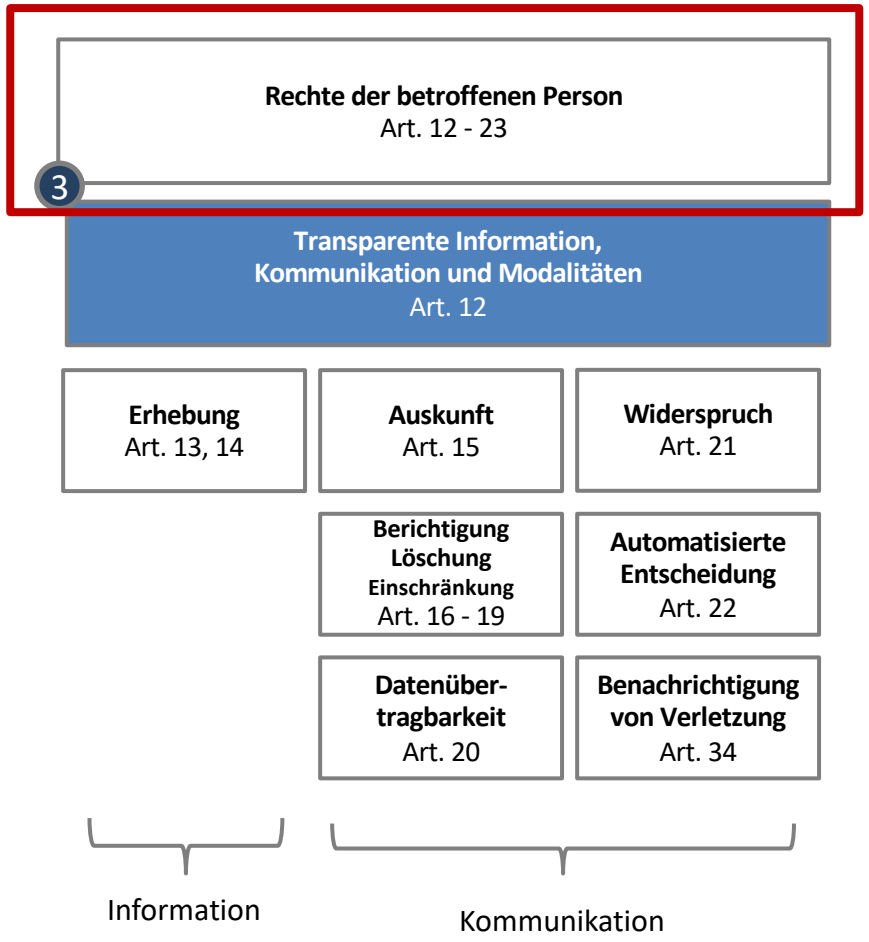
Quelle: Kranig, Sachs, Gierschmann:
Datenschutz-Compliance nach der DS-GVO, 2. Auflage, 2019

Art. 1 DS-GVO

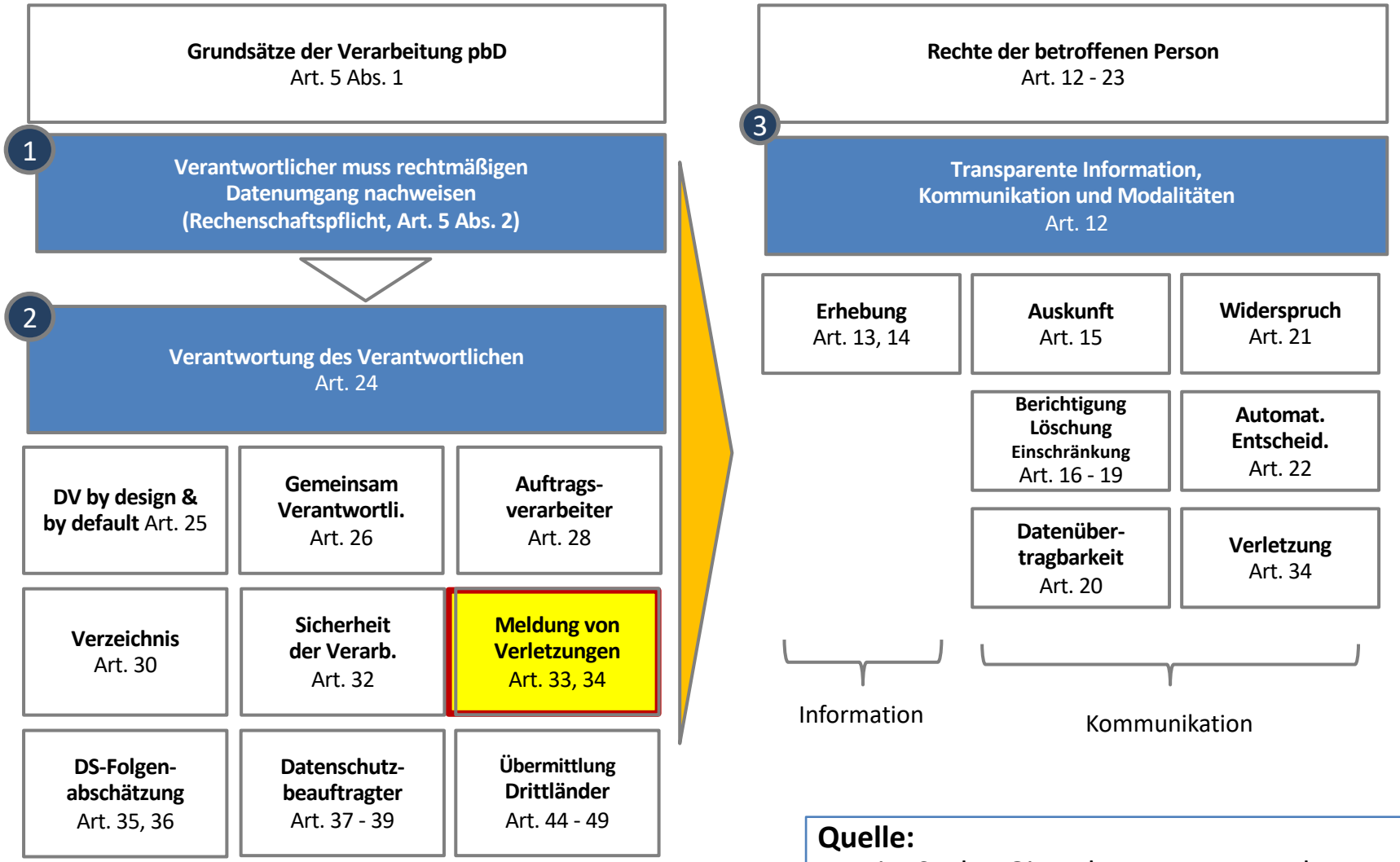
- Schutz der Grundrechte und Grundfreiheiten

und

- Freier Verkehr personenbezogener Daten



Quelle:
Kranig, Sachs, Gierschmann: Datenschutz-Compliance nach der DS-GVO, 2. Auflage, 2019



Quelle:
Kranig, Sachs, Gierschmann: Datenschutz-Compliance nach der DS-GVO, 2. Auflage, 2019

Art. 33 DS-GVO: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

[1]Im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, 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 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Art. 4 DS-GVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

12. „Verletzung des Schutzes personenbezogener Daten“ eine **Verletzung der Sicherheit**, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Art. 32 DS-GVO Sicherheit der Verarbeitung

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
   a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
   b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
   c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
   d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Art. 32 DS-GVO Sicherheit der Verarbeitung

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

d.h., wenn das gemacht wurde, kann von Sicherheit ausgegangen werden …

Working Paper 250 beschäftigt sich mit Verletzungen der Sicherheit

ARTIKEL-29-DATENSCHUTZGRUPPE

18/DE

WP250rev.01

Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

angenommen am 3. Oktober 2017

zuletzt überarbeitet und angenommen am 6. Februar 2018

Datenschutzverletzung – was ist das nun?

- Eine Verletzung des Schutzes personenbezogener Daten (kurz „Datenschutzverletzung“) ist gemäß Art. 4 Nr. 12 eine **Verletzung der Sicherheit**, die
  - ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung (**Verlust der Verfügbarkeit bzw. Integrität**) oder
  - zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten (**Verlust der Vertraulichkeit**) führt.

Vernichtung

Verlust

Veränderung

Unbeabsichtigt

Unrechtmäßig

Offenlegung

Zugang

Unbefugt

Wann besteht eine Meldepflicht bei der Aufsicht?

- **Grundsatz**:
  Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche diese der zuständigen Aufsichtsbehörde melden, Art. 33 Abs. 1 DS-GVO.

- **Ausnahme**:
  Der Verantwortliche hat feststellt, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führt (was zu dokumentieren ist, Art. 33 Abs. 5 DS-GVO).

Rahmenbedingungen für Meldung an Aufsichtsbehörde

- **Frist**: „unverzüglich und möglichst binnen 72 Stunden“
- **Inhalt**:
  - Kontaktdaten DSB
  - Beschreibung von: Art der Verletzung,
    - Kategorien, Anzahl Personen und Datensätze
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen
- **Dokumentation** der Verletzung
- Ergänzung möglich (Art. 33 Abs. 4 DS-GVO)

Rahmenbedingungen für die Erfüllung der Benachrichtigungspflicht gegenüber betroffenen Personen (Art. 34 DS-GVO)

- **Voraussetzung:** Hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen
- **Frist**: unverzüglich
- **Inhalt**: (*in klarer und einfacher Sprache*)
  - Beschreibung von:
    - Art der Verletzung,
    - Name und Kontaktdaten DSB
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen

Ausnahmen der Benachrichtigungspflicht (Art. 34 Abs. 3 DS-GVO)

- **Benachrichtigungspflicht gegenüber betroffenen Personen entfällt,**
  - wenn Verantwortlicher geeignete „und erfolgreiche“ technische und organisatorische Maßnahmen getroffen hat,
  - wenn er durch (der Verletzung) nachfolgende Maßnahmen das hohe Risiko reduziert hat oder
  - Benachrichtigung mit unverhältnismäßigem Aufwand verbunden wäre (dann aber ggfls. „öffentliche Bekanntmachung“ erforderlich).

Fall aus der Praxis

tagesschau.de

Startseite Videos & Audios

Startseite Investigativ

Patienteninformationen

Millionen Date

Stand: 17.09.2019 06:01 Uhr

Hochsensible medizinische Da
und den USA, sind nach Recher
ProPublica auf ungesicherten S

Von Maximilian Zierer und Hak

Die Nachrichten Politik Wirtschaft Wissen Kultur

Startseite › Informationen am Mittag › Offenbar Millione

Unsichere Server

Offenbar Millionen P
im Internet

Bundesdatenschützer Ulrich Kelber fordert
Datenschutzbehörden. Er reagiert damit auf
weltweit Millionen hochsensibler Patientend
Betroffen sind offenbar m

Von Arne Meyer-Fünffinge

Sensible Patientenda

BR

BR24 BR MEDIATHEK RADIO FERNSEHEN

BR.de › Fernsehen › BR Fernsehen › Münchner Runde › Röntgenbilder im Netz:

Röntgenbilder im Netz:

Wie sicher sind meine Gesundheitsdaten?

Hochsensible medizinische Patientendaten sind millionenfach frei zugänglich im Netz gelandet – darunter Röntgenbilder und Brustkrebsscreenings. Wie gefährlich ist das? Wie schützen wir Patientendaten und sorgen gleichzeitig für eine vernünftige Digitalisierung in der Medizin?

Stand: 30.09.2019 | Bildnachweis

ZDF heute

Röntgenbilder und MRT-Aufnahmen

Millionen Patientendaten ungeschützt im Netz

17.09.2019 17:59 Uhr

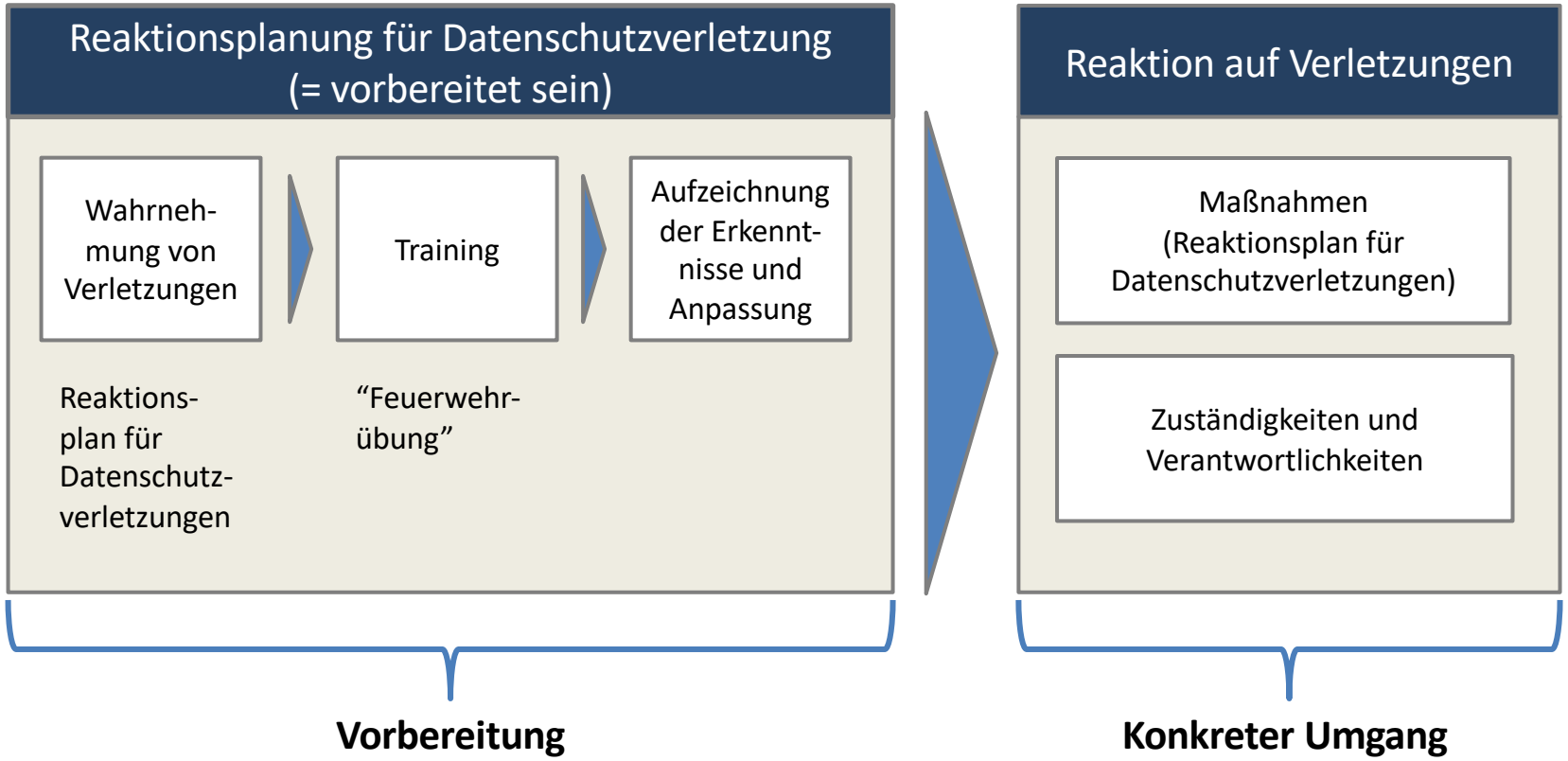
Es ist eine gravierende Sicherheitslücke: Millionen Patientendaten standen offenbar jahrelang ungeschützt im Netz. Es geht unter anderem um Röntgenbilder und MRT-Aufnahmen.

- **Was war passiert?**
  - Arzt hat bei Rechner …
  - Bayer. Rundfunk u.a. haben das entdeckt und ... informiert (nicht BayLDA)
  - BayLDA wurde von Rechtsanwalt einer nicht betroffenen Klinik informiert.
  - BayLDA hat Gerät bzw. Verantwortlichen ermittelt und veranlasst, dass Lücke geschlossen wird.
  - Verantwortlicher hat (innerhalb von 72 Std.) Meldung nach Art. 33 DS-GVO abgesetzt.
  - BayLDA hat Rechner (im Einvernehmen mit Verantwortlichem) forensisch untersucht und keine Anhaltspunkte für Zugriffe außer von Journalisten und BayLDA entdeckt.

- **Was hat BayLDA gemacht?**
  - BayLDA hat Vorgang intensiv geprüft und - wie Verantwortlicher - den Vorfall nicht als „hohes Risiko für Patienten“ gemäß Art. 34 DS-GVO bewertet.
  - BayLDA hat kein OWi-Verfahren eingeleitet.

Vorbereitungs- bzw. Ablaufplan für Datenschutzverletzungen

ErwGr. 87: *Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können*



Quelle:
Kranig, Sachs, Gierschmann: Datenschutz-Compliance nach der DS-GVO, 2. Auflage, 2019

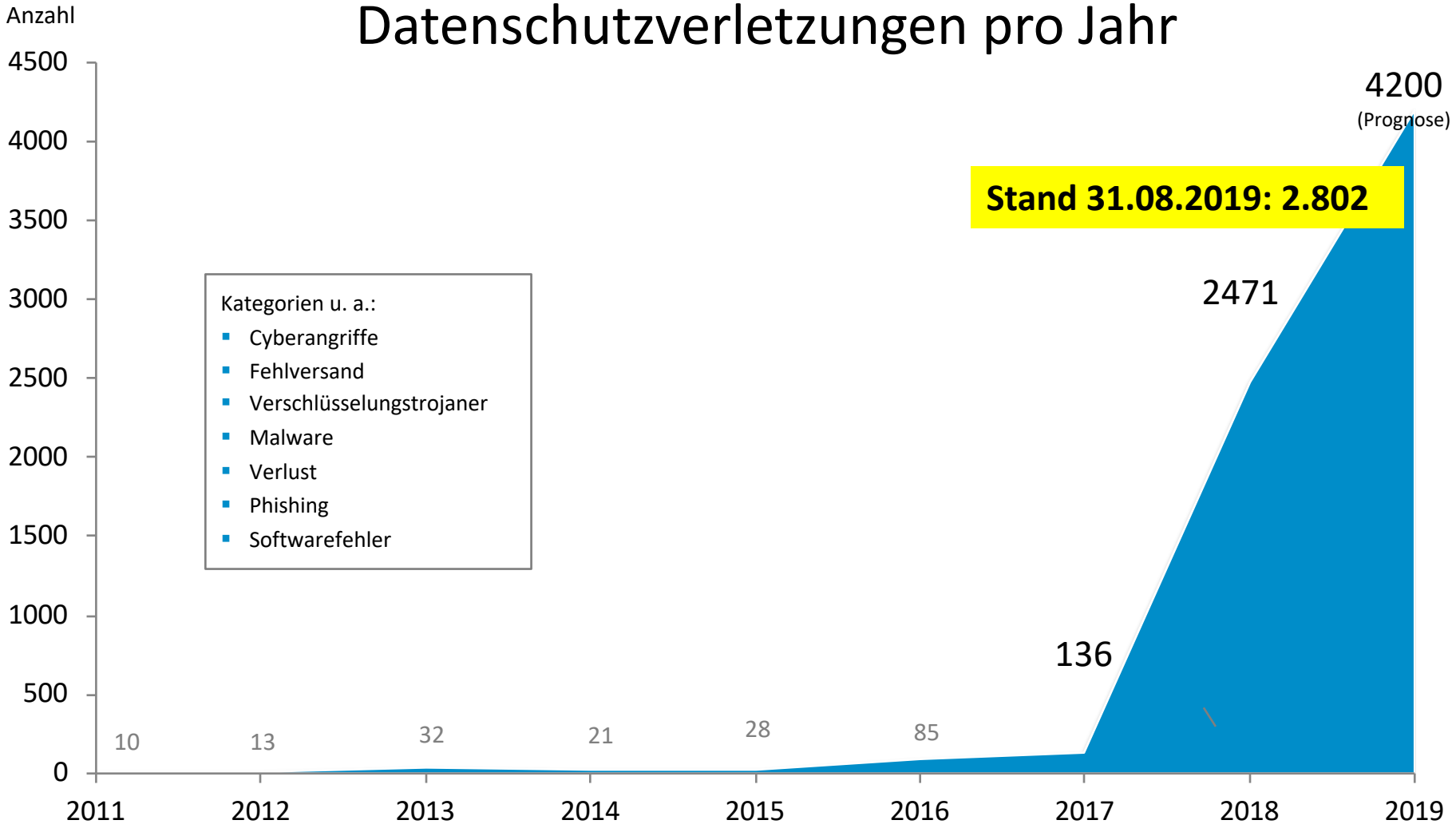
Agenda

1. Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?
2. **Meldeverhalten in Deutschland und Europa**
3. Wie geht die Aufsicht mit den Meldungen um?
4. Art. 33 DS-GVO und Geldbuße – geht das?
5. Ausblick

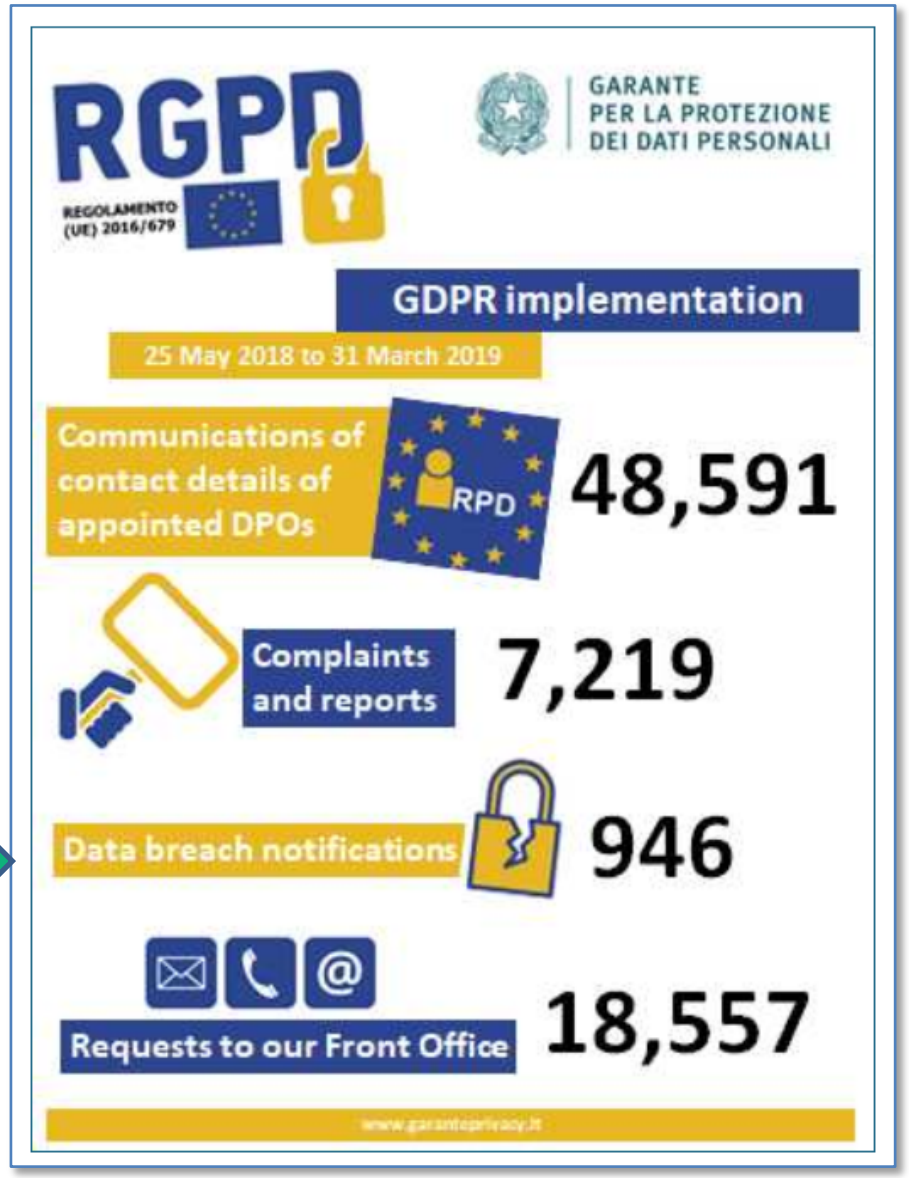
Meldung von Datenschutzverletzungen bei einigen deutschen Aufsichtsbehörden

AB	Zahl ges.	25.05. - 31.12.18	öffentl. Bereich	n.-öff. Bereich	01.01. - 30.06.19	öffentl. Bereich	n.-öff. Bereich
1	11418	6114	5758	356	5304	4929	375
2	5235	2776	400	2376	2029		2029
3	299	124	62	62	175	103	72
4	1386	629	91	538	757	93	641
5	762	382	108	274	380	134	246
6	2395	1197			1198		
7	233	77	14	63	156	33	123
8	452	227	35	192	225	60	165
9	127	53			74		
10	293	126	31	95	167	41	126

Datenschutzverletzungen pro Jahr

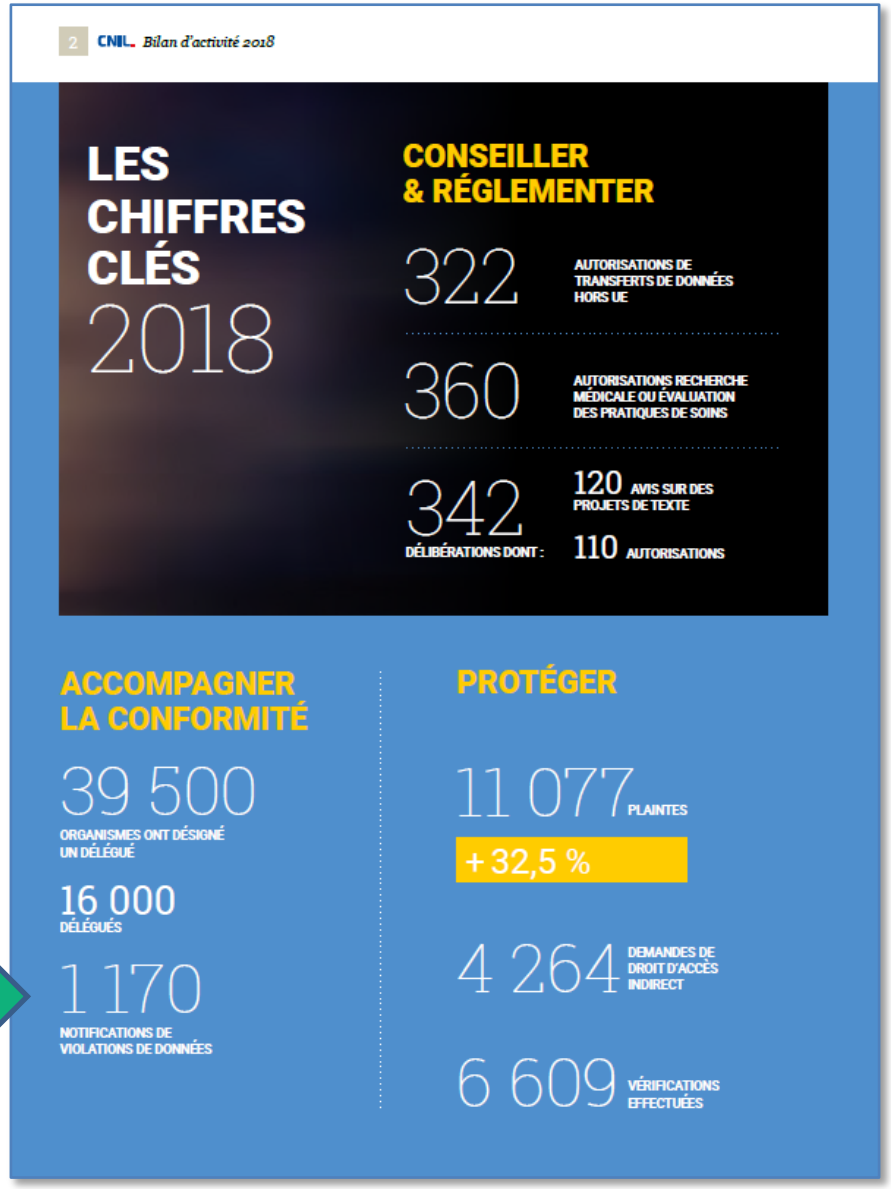


GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



https://www.garanteprivacy.it/web/guest/home_en

CNIL.



https://www.cnil.fr/en/presentation-2018-activity-report-and-2019-issues-french-data-protection-authority

… da stimmt etwas nicht !!

	Number of notifi-cations to authority	Period
	290	May 18 – Jan 19
	946	May 18 - Mar 19
	547	May 18 - Dec 18
	1.170	May 18 - Mar 19
	4.200	May 18 - Mar 19

Es ist noch ein großes und notwendiges Stück Arbeit, bis wir Aufsichtsbehörden in Europa die **Art. 33 und 34 DS-GVO** und die **Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679** einheitlich verstehen.

Wir arbeiten daran !!

ARTIKEL-29-DATENSCHUTZGRUPPE

18/DE

WP250rev.01

Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

angenommen am 3. Oktober 2017

zuletzt überarbeitet und angenommen am 6. Februar 2018

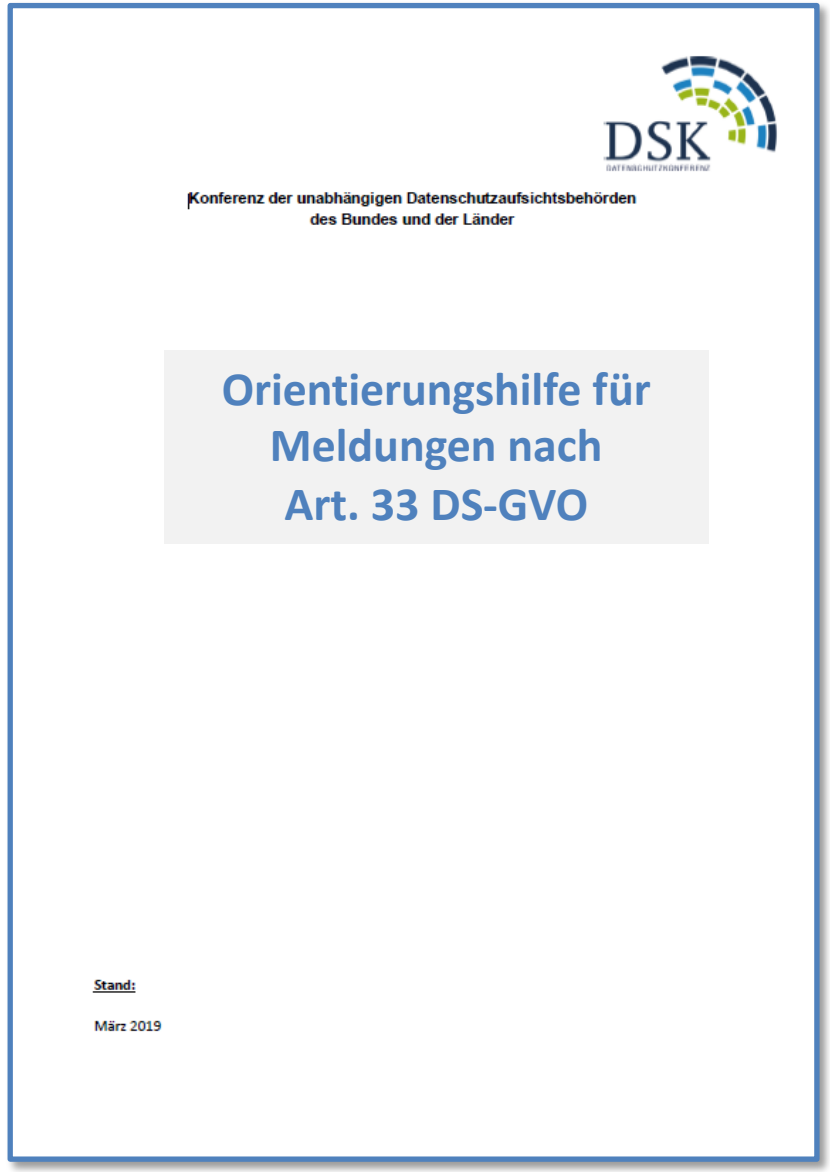
Diese Gruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtet. Sie ist ein unabhängiges europäisches Beratungsgremium für den Schutz personenbezogener Daten und der Privatsphäre. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Das Sekretariat wird von der Direktion C (Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, Generaldirektion für Justiz, B-1049 Brüssel, Belgien, Büro MO-59 02/013, gestellt.

Website: http://ec.europa.eu/justice/data-protection/index_de.htm

Wir arbeiten daran !!

DSK hat **Task Force „Meldekriterien nach Art. 33 DS-GVO**“ gegründet.
Ziel ist, einheitlichere Kriterien für Meldungen zu erarbeiten, diese in Deutschland abzustimmen und dann damit nach Europa zu gehen.


DSK

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Orientierungshilfe für Meldungen nach Art. 33 DS-GVO

Stand:

März 2019

Agenda

1. Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?
2. Meldeverhalten in Deutschland und Europa
3. **Wie geht die Aufsicht mit den Meldungen um?**
4. Art. 33 DS-GVO und Geldbuße – geht das?
5. Ausblick

Wie kann BayLDA mit dieser Menge an Meldungen umgehen?

Brief / Fax

5 %

Online-Service

95 %

Internes Verwaltungs-system

Fehlversand → Risiko-validierung → (Abschluss-) Schreiben

Hoher Automatisierungs-grad

Hacking
Softwarefehler
Verlust
…

Scoring (Fokus: Risiko)

Sachbearbeiter

Hoher Score: Reporting

Sehr hoher Score

Referatsleiter

(Abschluss-) Schreiben

Ggf.

Weitere Kontrollen

Ggf.

Bußgelder

Unser (BayLDA) Ziel:
Jede Meldung nach Art. 33 DS-GVO muss bearbeitet und beantwortet werden

Wie kann LfDI BW mit dieser Menge an Meldungen umgehen?

- Anzahl der Meldungen von Datenpannen haben sich seit Mai 2018 **verzehnfacht**
- **Seit 1.1.2019 1.400 Meldungen**
- **Häufigste Konstellationen:**
  - Fehlversand von Post/E-Mail/Fax
  - Hackingangriffe/Malware/Trojaner
  - Diebstahl/Verlust eines Datenträgers
  - Versendung einer E-Mail mit offenem Adressverteiler
- Auffällige **Häufung**: Arztpraxen
- Besonderes **Problem**: Verschlüsselungstrojaner

Agenda

1. Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?
2. Meldeverhalten in Deutschland und Europa
3. Wie geht die Aufsicht mit den Meldungen um?
4. **Art. 33 DS-GVO und Geldbuße – geht das?**
5. Ausblick

Sanktioniert BayLDA gem. Art. 33 DS-GVO gemeldete Verstöße?

- **NEIN:** **(z. Zt.) keine Geldbuße bei mitgeteilten Verstößen geplant**
  - § 43 Abs. 4 BDSG (neu)

    Eine Meldung nach **Artikel 33** der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 **darf in** einem Verfahren nach dem Gesetz über **Ordnungswidrigkeiten** gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen **nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.**

- **ABER:** Gilt nur für gemeldeten Sachverhalt, nicht für Erkenntnisse, die BayLDA im Zuge ergänzender Prüfungen erfährt

Sanktioniert LDI BW gem. Art. 33 DS-GVO gemeldete Verstöße?

- Ja
  - § 43 Abs. 4 BDSG kein anwendbares Recht

- **Höchste Sanktionen: 2 & 80.000 €**

- **Konstellationen:**
  - digitale Publikation von Gesundheitsdaten
  - Unternehmen aus der Finanzwirtschaft entsorgt personenbezogene Daten unsachgemäß

Agenda

1. Art. 33 DS-GVO - Was will uns diese Vorschrift sagen?
2. Meldeverhalten in Deutschland und Europa
3. Wie geht die Aufsicht mit den Meldungen um?
4. Art. 33 DS-GVO und Geldbuße – geht das?
5. **Ausblick**

- **Verständnis von meldepflichtigen Vorfällen muss vereinheitlicht werden**
  - UAK der DSK (Leitung BayLDA) soll Kriterienkatalog für Meldepflicht ja oder nein entwerfen (offen für Anregungen aus der Wirtschaft – bitte an Aufsichtsbehörden melden)
  - DSK kann dann Kriterienkatalog nach Europa transportieren
- **Entscheidung, ob Art. 83 DS-GVO Anwendungsvorrang vor § 43 BDSG hat, soll schnell herbeigeführt werden**
  - Wenn Aufsichtsbehörde meint, das sei so, dann sollte sie einen Musterfall herausgreifen und eine Geldbuße verhängen.

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen zum Datenschutz und zur Informationsfreiheit finden Sie auf unseren Webseiten

www.baden-wuerttemberg.datenschutz.de

und

www.lda.bayern.de