LawCamp

Vorgehen vor, während und nach Data Breaches & Bird & Bird

Dr. Simon Assion, CIPP/E

IT LawCamp 2019

16.11.2019 in den Design Offices Frankfurt

Übersicht

1. Vorbereitung

2. Vorgehen bei Verstößen

3. Nachbereitung

LawCamp

Bird & Bird

1. Vorbereitungen

Bird & Bird

Bevor etwas passiert

LawCamp

Bird & Bird

Technische Vorbereitung

- Allgemein: **ISMS**, ausgerichtet nach Risikoklassen
- **Zur Erkennung: SIEM**
  - (Security Information and Event Management)

LawCamp

Bird & Bird

Einige Beispiele:

- Sicherheitsrollen und Verantwortlichkeiten
- Vendor Management
- Sicherheitsüberprüfung im Personalmanagement
- Patch Management
- Password Policy, 2FA
- Physische Zugangskontrollen
- Mitarbeiterschulungen, Sensibilisierung
- Notfallübungen

LawCamp

Bird & Bird

Organisatorische Vorbereitung

- **Schulung der Mitarbeiter*innen:**
  - Was tun? (Netzstecker ziehen?)
  - Was melden?
  - Wem melden?
  - Wann, bzw. wie schnell melden?
- **Vorgefertigte Ablaufpläne**
  - ("Standard Operating Procedures")
- **Zusammenstellung eines Krisen-Reaktionsteams**
- **Etablierung von Kontakten zu externen Beratern**
  - Anwälte, PR, IT-Forensik, evtl. internal Investigations

LawCamp

Bird & Bird

Das Krisenreaktionsteam

1) **CSO**
2) **IT** (CSIRT / CERT)
3) **DPO**
4) **Legal**
5) **HR**
   - Falls Sanktionen gegen Beschäftigte
   - Falls interne Untersuchungen notwendig
4) **Evtl. Compliance-Beauftragte*r**
5) **Presseabteilung**
   - Krisen-PR
   - Information der Betroffenen

LawCamp

Bird & Bird

2. Vorgehen bei Verstößen

Bird & Bird

Meldepflicht?
Art. 4 Nr. 12 DSGVO

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

LawCamp

Bird & Bird

Verletzung der Sicherheit?

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

Achtung: Meldepflichten (mit anderen "Auslösern") können auch aus anderen Gründen entstehen, z.B.:

- Vertrag
- § 80 BetrVG
- §§ 109, 109a TKG
- §§ 8b, 8c BSIG
- § 54 ZAG

LawCamp

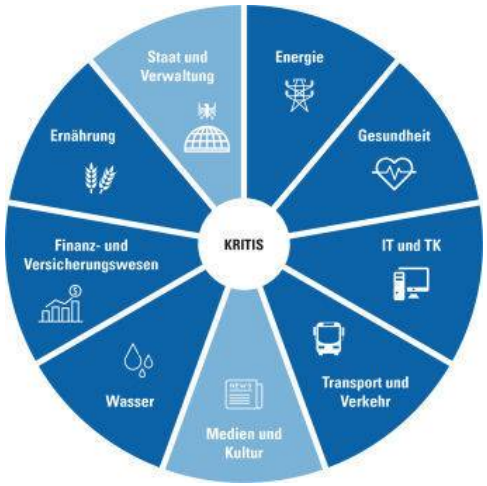
Bird & Bird

Meldepflichten außerhalb der DSGVO

BSIG

Digitale Dienste:

- Suchmaschinen, Marktplätze, Cloud-Computing



KRITIS (Beispiele):

- **Telekommunikation**
  - Ortsgebundene Zugangsnetze
  - Übertragungsnetze
  - Rechenzentren, Serverfarmen
- **Energie**
  - Erzeugungs- und Speicherungsanlagen
- **Finanz- und Versicherungswesen**
  - IT-Systeme für Cash Management, Auszahlungssysteme, System zur Aufbereitung von Zahlungsanweisungen

LawCamp

Bird & Bird

Meldepflichten außerhalb der DSGVO

Meldepflicht an das BSI bei "Störungen"

Störung

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,
2. Erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Meldepflichten außerhalb der DS-GVO: BSIG

BSIG

Inhalt der Meldung

- Angaben zu der Störung,
- möglichen grenzübergreifenden Auswirkungen,
- technischen Rahmenbedingungen,
- Ursache,
- Informationstechnik,
- Art der Einrichtung oder Anlage,
- erbrachte kritische Dienstleistung und Auswirkungen der Störung für diese Dienstleistung;
- ggf. Betreiber

Meldepflichten außerhalb der DSGVO: TKG

Anwendungsbereich (§§ 109, 109a TKG):

- Anbieter öffentlich zugänglicher Telekommunikationsdienste
- Betreiber öffentlicher Telekommunikationsnetze

Meldung an die Betroffenen (§ 109a Abs. 2 S. 1 TKG)

1. Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

Meldung an die BNetzA und den BfDI (§ 109a Abs. 2 S. 2 TKG)

- Nr. 1-3
- Folgen der Verletzung des Schutzes personenbezogener Daten
- Beabsichtigte oder ergriffene Maßnahmen

LawCamp

Bird & Bird

Meldepflichten außerhalb der DSGVO: ZAG

Meldung schwerwiegender Betriebs- oder Sicherheitsvorfälle § 54 Abs. 1 ZAG

- Regulierte Zahlungsdienstleister
- Schwerwiegender Betriebs- oder Sicherheitsvorfall
  - "einzelnes Ereignis, oder eine Reihe zusammenhängender Ereignisse, das vom Zahlungsdienstleister nicht beabsichtigt wurde und das sich negativ auf die Integrität, die Verfügbarkeit, die Vertraulichkeit, die Authentizität und/oder die Kontinuität von zahlungsbezogenen Diensten auswirkt oder aller Wahrscheinlichkeit nach eine solche negative Auswirkung haben wird."
    BaFin Rundschreiben 08/2018 (BA) zur Meldung schwerwiegender Zahlungssicherheitsvorfälle

LawCamp

Bird & Bird

Meldepflichten außerhalb der DSGVO

BetrVG

- Information des Betriebsrats § 80 (1), Nr. 1, (2) BetrVG

> § 80 Allgemeine Aufgaben
> (1) Der Betriebsrat hat folgende allgemeine Aufgaben:
> 1. darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden; [...]
> (2) Zur Durchführung seiner Aufgaben nach diesem Gesetz ist der Betriebsrat **rechtzeitig und umfassend vom Arbeitgeber zu unterrichten**; die Unterrichtung erstreckt sich auch auf die Beschäftigung von Personen, die nicht in einem Arbeitsverhältnis zum Arbeitgeber stehen, und umfasst insbesondere den zeitlichen Umfang des Einsatzes, den Einsatzort und die Arbeitsaufgaben dieser Personen. [...]

- Information des Wirtschaftsausschusses § 106 (2), (3) Nr. 10 BetrVG
  - Sofern Interessen des Arbeitnehmers wesentlich berührt werden könnten.

Meldepflichten außerhalb der DSGVO: SGB X

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten § 83a SGB X

- Stellen, die den Sozialgeheimnis unterliegen (§ 35 SGB I)

  - u.a. Verbände und Arbeitsgemeinschaften der Leistungsträger, Datenstelle der Rentenversicherung, sonstige in SGB I genannten öffentlich-rechtlichen Vereinigungen, Integrationsfachdienste, Versicherungsämter

- Meldepflicht
  - Meldung an die Rechts- oder Fachaufsichtsbehörde

LawCamp

Bird & Bird

Definition der Datenschutzverletzung (DSGVO)

Im Detail: Art. 4 Nr. 12 DSGVO

Was?

- Nur in Bezug auf personenbezogene Daten

Wann? Bei:

- Verletzung der Sicherheit, mit der Folge:
  - Vernichtung
  - Verlust
  - Veränderung
  - Unbefugte Offenlegung bzw. unbefugter Zugang

LawCamp

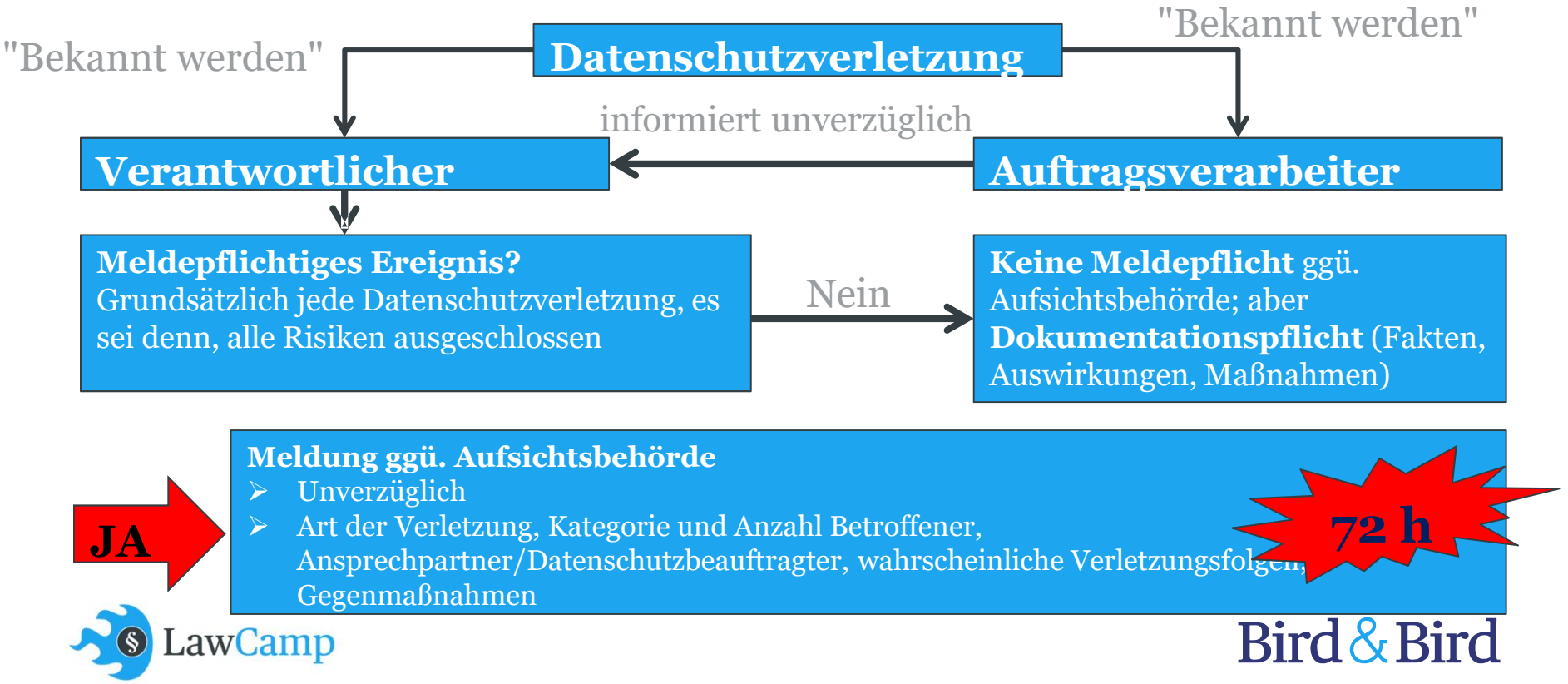
Bird & Bird

Meldepflichten bei Datenschutzverletzungen

LawCamp

Bird & Bird

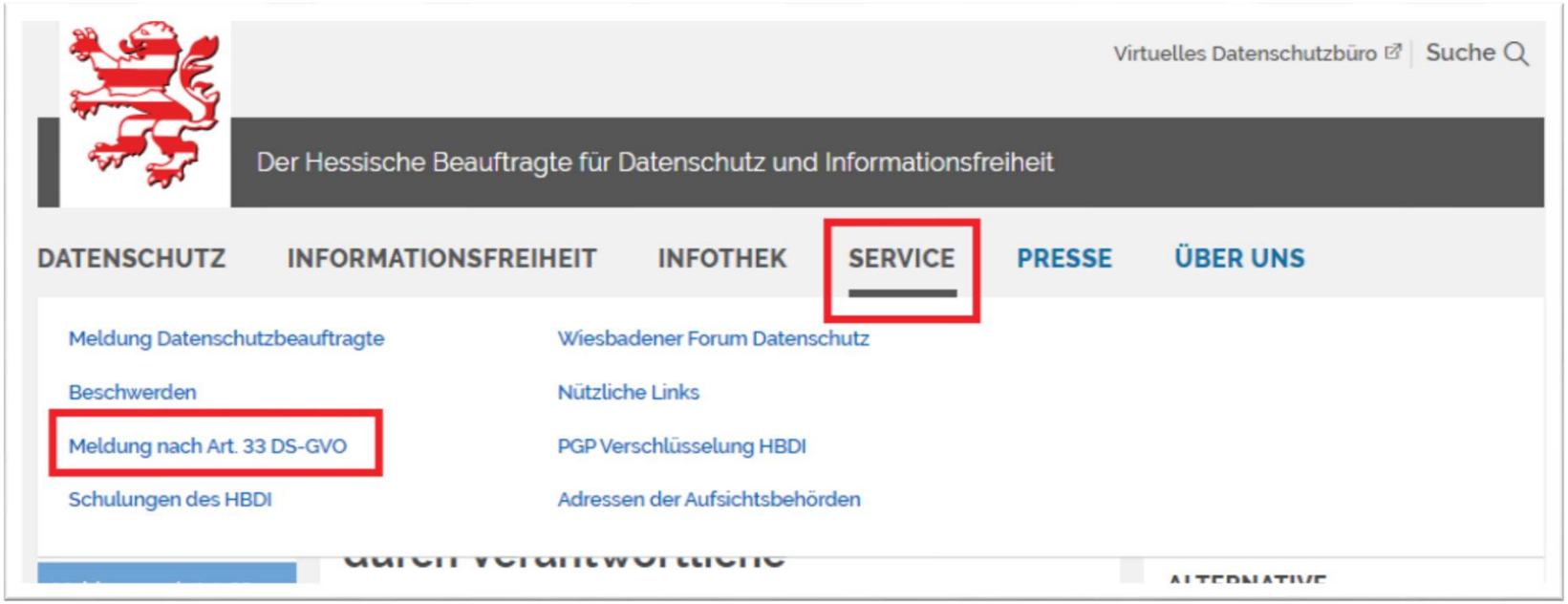
Meldepflicht an Aufsichtsbehörde, Art. 33



LawCamp

Bird & Bird

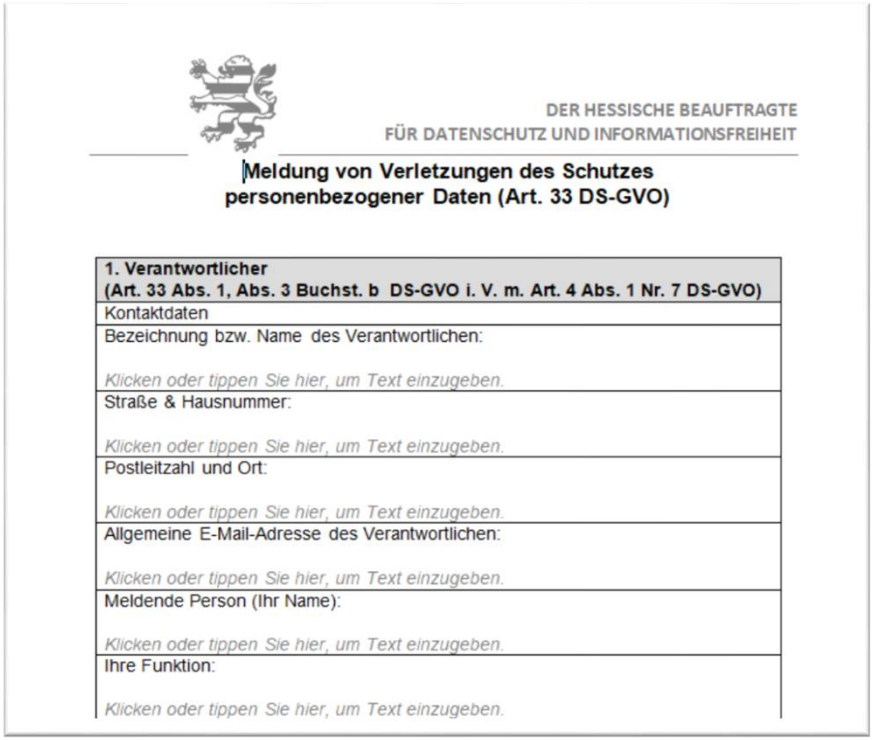
Meldung eines Datenschutzvorfalls in Hessen



LawCamp

Bird & Bird

Meldung eines Datenschutzvorfalls in Hessen



DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

1. Verantwortlicher (Art. 33 Abs. 1, Abs. 3 Buchst. b DS-GVO i. V. m. Art. 4 Abs. 1 Nr. 7 DS-GVO)
Kontaktdaten
Bezeichnung bzw. Name des Verantwortlichen: *Klicken oder tippen Sie hier, um Text einzugeben.*
Straße & Hausnummer: *Klicken oder tippen Sie hier, um Text einzugeben.*
Postleitzahl und Ort: *Klicken oder tippen Sie hier, um Text einzugeben.*
Allgemeine E-Mail-Adresse des Verantwortlichen: *Klicken oder tippen Sie hier, um Text einzugeben.*
Meldende Person (Ihr Name): *Klicken oder tippen Sie hier, um Text einzugeben.*
Ihre Funktion: *Klicken oder tippen Sie hier, um Text einzugeben.*

LawCamp

Bird & Bird

Wie vermeidet man Sanktionen?

Die ungeschriebene "Phase 0" des DSK-Bußgeldkonzepts:

Sachbearbeiter*in der Aufsichtsbehörde prüft, ob er den Vorgang in die Bußgeldabteilung abgibt.

Wann wird sie/er dies tun?

- Wenn der Eindruck entsteht, dass Fehler "System hat" (z.B. zur Gewinnerzielung)
- Wenn Eindruck entsteht, dass der Verantwortliche es ohne Bußgeld "nicht lernt"
- Wenn hohe Schäden bzw. viele Betroffene

LawCamp

Bird & Bird

Was also tun?

- **Schnell handeln**
  - (72 h nicht unbedingt ausnutzen)
- **Ursache der Sicherheitsverletzung sofort abstellen**
  - Erfordert bei nicht-evidenter Ursache i.d.R. IT-forensische Untersuchung
- **Folgen der Verletzung maximal möglich eindämmen**
  - **Betroffene informieren** (auch wenn man nicht muss!)
  - **Erklären, was nun zu tun ist** (z.B. Passwörter ändern, Beschreiben wie man Phishing-Angriffe erkennt)
  - **Hilfemaßnahmen anbieten** (z.B. Kreditmonitoring)
  - Falls notwendig: **Daten zurückerlangen**, **Wiederveröffentlichung verhindern**
- **Sofort mit Überarbeitung der TOMs beginnen**

LawCamp

Bird & Bird

Wie informiere ich die Betroffenen

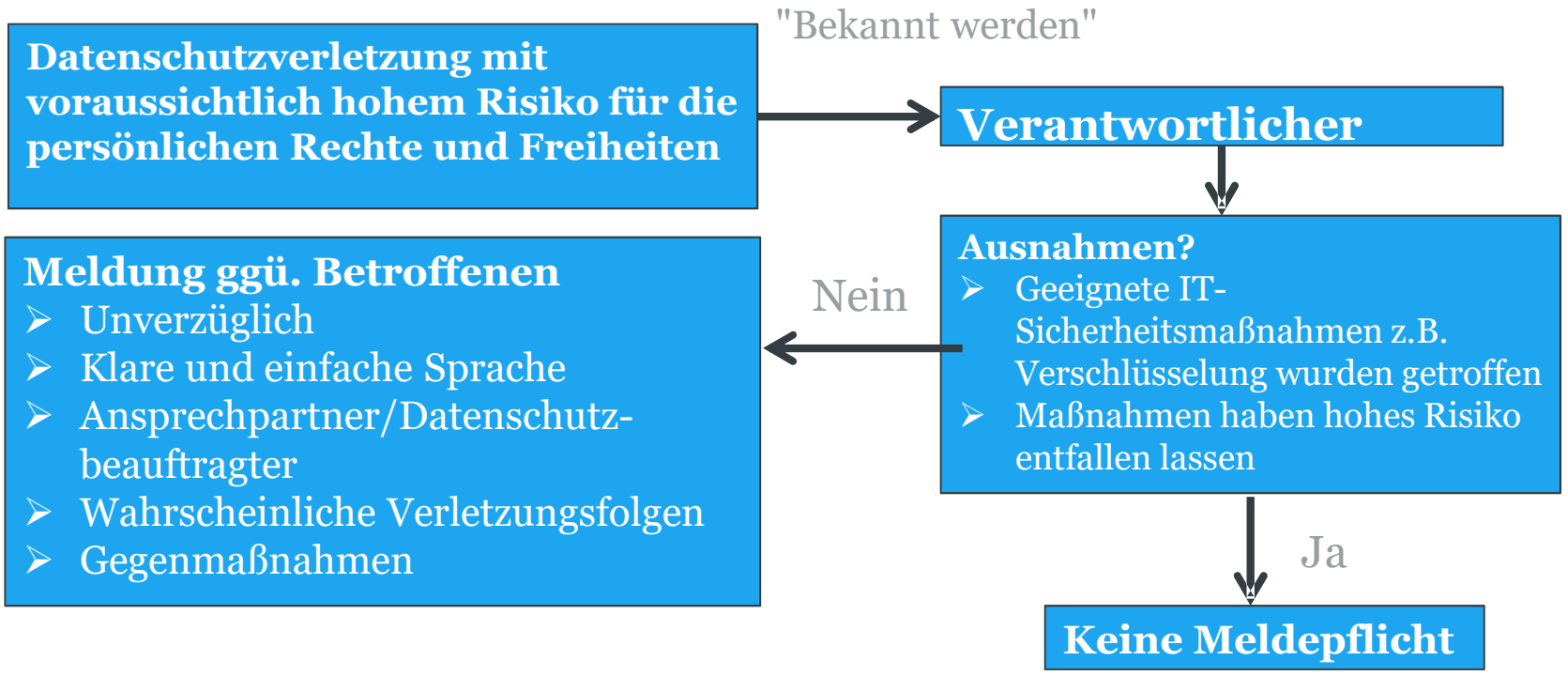
"Best case": Sofort und trotzdem vollständig (Art. 34 DSGVO)

- **Unmöglich? Nicht immer!**
- Die Meldung an die Betroffenen sollte kombiniert werden mit:
  - **Kontaktmöglichkeit (z.B. Hotline)**
  - **Link auf FAQ im Internet** (die nachträglich angepasst werden können!)
- Unbedingt aber vermeiden: **"Scheibchenweise" Information der Betroffenen**
  - (sonst: "das wird ja immer schlimmer" / "die haben die Kontrolle verloren")

LawCamp

Bird & Bird

Mitteilung an die Betroffenen, Art. 34



LawCamp

Bird & Bird

Meldepflichten außerhalb der DS-GVO

- **§§ 8b, 8c BSIG**
- **§§ 109 109a TKG**
- **§ 54 Abs. 1 ZAG**
- **§ 83a SGB X**
- **§ 80 Abs. 1 Nr. 1, Abs. 2 BetrVG**
- **§ 106 Abs. 2, Abs. 3 Nr. 10 BetrVG**

LawCamp

Bird & Bird

3. Nachbereitung von Verstößen

Bird & Bird

Plan-Do-Check-Act

Wo waren die bestehenden Sicherheitsmaßnahmen nicht ausreichend?
Wo können sie verbessert werden?

Beispiele:

- Überarbeitung von Mitarbeiterschulungen
- Einführung von SIEM
- Einführung von (Quellen-) Verschlüsselung
- Zusätzliches Hashing/Pseudonymisierung
- Einführung von 2FA

Mit der Datenschutzbehörde!

LawCamp

Bird & Bird

Bußgeldverfahren

Allgemein

Einleitung von Bußgeldverfahren nach Meldung von Datenschutzverletzungen ist nichts Ungewöhnliches.

Aber: Die Meldung indiziert keinen Verstoß gegen die DSGVO!

Def.:

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

"Verletzung der DSGVO" kommt nicht vor.

LawCamp

Bird & Bird

Bußgeldverfahren

Nemo tenetur?

- § 42 (4) BDSG
  - "Eine Meldung nach Art. 33 DSGVO [...] darf in einem Strafverfahren gegen den Meldepflichtigen [...] nur mit Zustimmung des Meldepflichtigen [...] verwendet werden."
  - Gleiches gilt für den Benachrichtigenden nach Art. 34 DSGVO

Anwendbarkeit auf Unternehmen ggf. unionsrechtswidrig (str.!)

- Nach dem EuGH besteht im Kartellrecht für Unternehmen nur ein "Geständnisverweigerungsrecht"
- Bislang ist § 42 (4) BDSG jedoch geltendes Recht

LawCamp

Bird & Bird

Bußgeldverfahren

Vermeidung hoher Bußgelder

Selbständige Benachrichtigung der Datenschutzaufsicht

- Höhe des Bußgelds von der Art und Weise der Kenntniserlangung der Aufsichtsbehörde abhängig (Art. 83 (2), S. 2, lit. h DSGVO)

Kooperation ist mildernd zu berücksichtigen (Art. 83 (2), S. 2, lit. f)

- Sonst Verstoß gegen die Verhältnismäßigkeit des Bußgelds aus Art. 83 (1)

50 %

Schnelle Behebung der Datenpanne geboten

- Höhe des Bußgelds ist auch von der Dauer des Verstoßes abhängig (Art. 83 (2), S.2, lit. a)

Sonstige kooperative Verhaltensweisen (Art. 83 (2), S. 2, lit. k)

LawCamp

Bird & Bird

Bußgeldverfahren
Verjährung

Nach § 41 (2) BDSG ist das OWiG auf das Bußgeldverfahren anzuwenden.

Verjährung der Verstöße nach § 31 ff. OWiG:

- Spätestens Verjährung nach **3 Jahren** § 31 (2) Nr. 1 OWiG (ab einer Geldbuße von mehr als 15.000 EUR)
- Verjährungsbeginn bei Beseitigung des Verstoßes (Datenschutzverstöße sind Dauerdelikte i.S.d. § 31 (3) S. 1 OWiG)

Sonstige Risiken nach Data Breaches

Schadensersatz-/Entschädigungsanspruch des Betroffenen gegen den Verantwortlichen (Art. 82 DSGVO und § 83 BDSG)

- Verschuldensunabhängig (?)
- Einwendung nach Art. 82 (3) DSGVO

Führen Sicherheitsverletzungen zu Schadensersatz- oder Unterlassungsansprüchen?

- Schadensersatz (h.M.): Nicht bei Bagatellschäden
- Unterlassungsansprüche: Strittig

- Wann kommt die erste **Musterfeststellungsklage** nach einem Data Breach?

LawCamp

Bird & Bird

Fazit

Be Prepared... the meaning of the motto is that a scout must prepare himself by previous thinking out and practicing how to act on any accident or emergency so that he is never taken by surprise.

(Robert Baden-Powell)

LawCamp

Bird & Bird

Thank you & Bird & Bird

Dr. Simon Assion
Tel. +49 (0)69 74222 6560
simon.assion@twobirds.com

twobirds.com