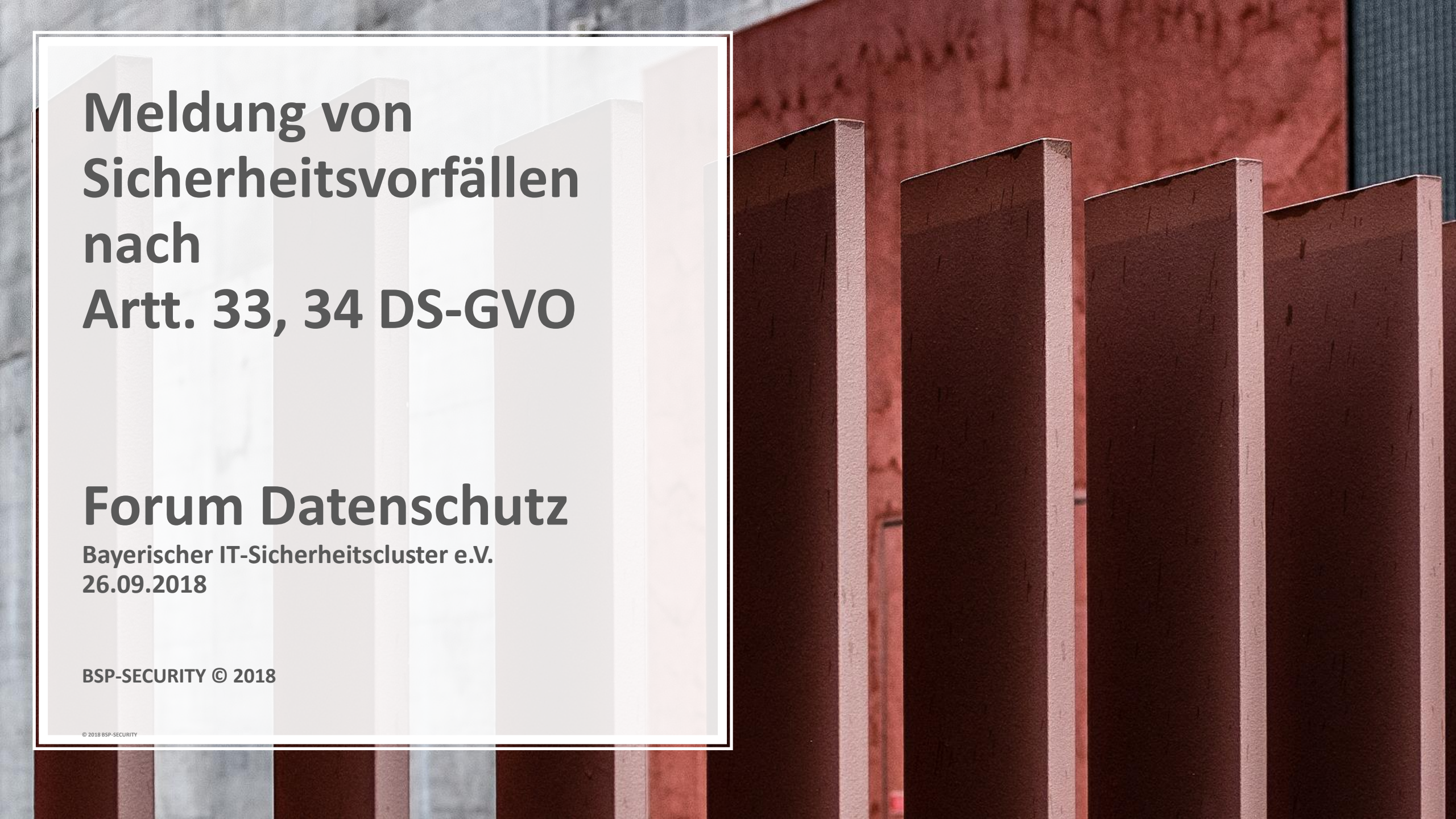


Meldung von Sicherheitsvorfällen nach Artt. 33, 34 DS-GVO

Forum Datenschutz

Bayerischer IT-Sicherheitscluster e.V.
26.09.2018

Michael Gruber

Berater IT-Compliance (Datenschutz und Informationssicherheit)

Fachbeirat Datenschutz Bayerischer IT- Sicherheitscluster e.V.

ISIS12 Initiator und Architekt

BSP-SECURITY

1 Was ist ein meldepflichtiger Sicherheitsvorfall?

1 Was ist ein meldepflichtiger Sicherheitsvorfall?

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.

(Art. 33 DS-GVO)

BSP-SECURITY

1 Was ist ein meldepflichtiger Sicherheitsvorfall?

Was ist damit konkret gemeint?

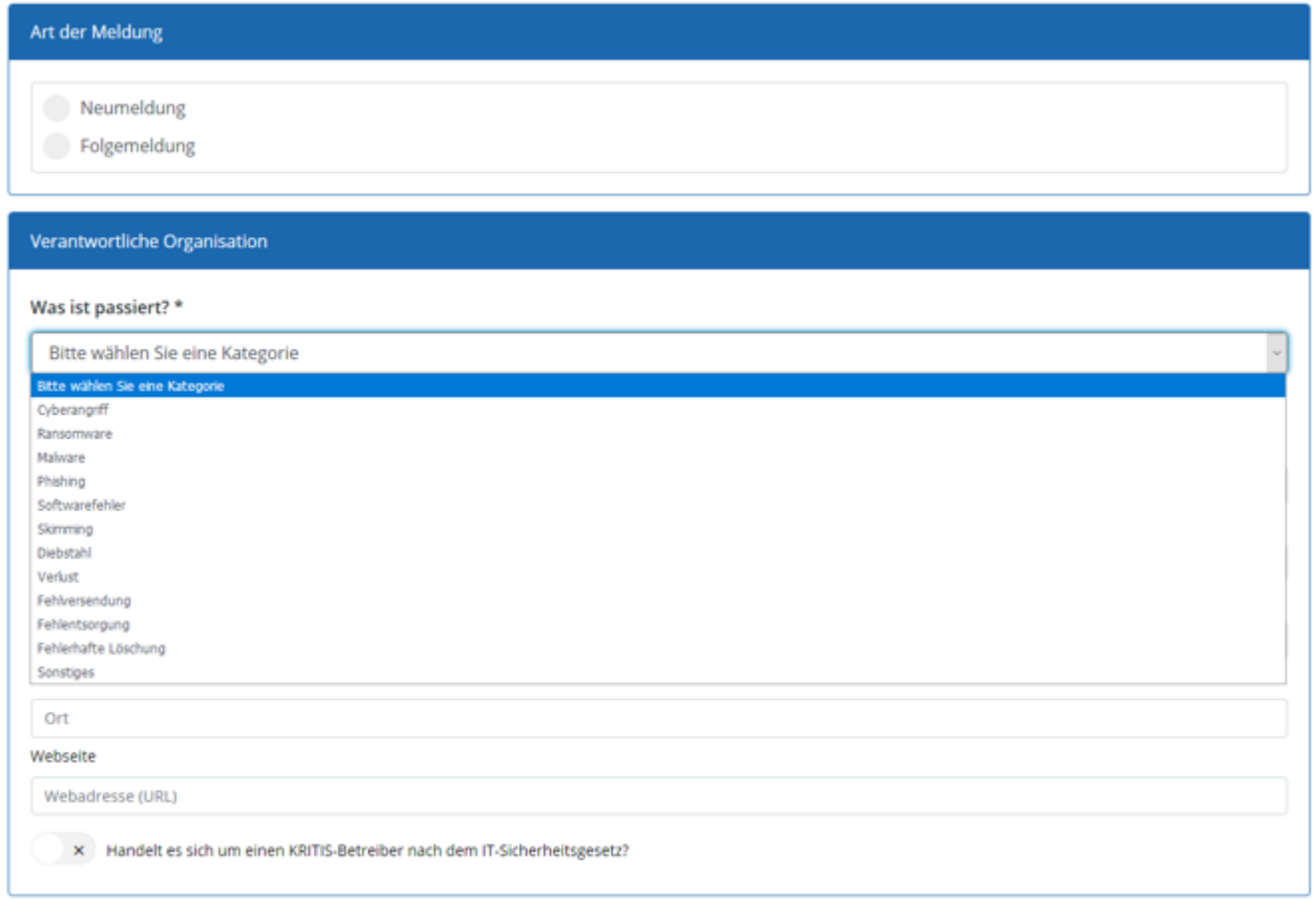
Welche Ereignisse fallen darunter?

Beispiele:

- **Verlorenes/gestohlenes Notebook, Smartphone …**
- **Fehlgeleitete E-Mail an Unberechtigte**
- **Malware**
- **Einbruch**
- **Erfolgreiches Hacking**
- **…**

BSP-SECURITY

1 Was ist ein meldepflichtiger Sicherheitsvorfall?



https://www.lda.bayern.de/de/datenpanne.html

BSP-SECURITY

we make security simple.

2 Wer muss informiert werden?

2 Wer muss informiert werden?

- ***Risiko* für den Betroffenen:**
  Zuständige Datenschutzaufsichtsbehörde (Art. 33 DS-GVO)

  Online-Meldung:
  https://www.lda.bayern.de/de/datenpanne.html

- ***Hohes Risiko* für den Betroffenen:**
  Der oder die Betroffenen (Art. 34 DS-GVO) mit Ausnahmen (Abs. 3)

- **Wen hat der *Auftragsverarbeiter* zu informieren? (Art. 28 DS-GVO)**

  Den Verantwortlichen (Auftraggeber)

BSP-SECURITY

3 Vorgehen in der Praxis

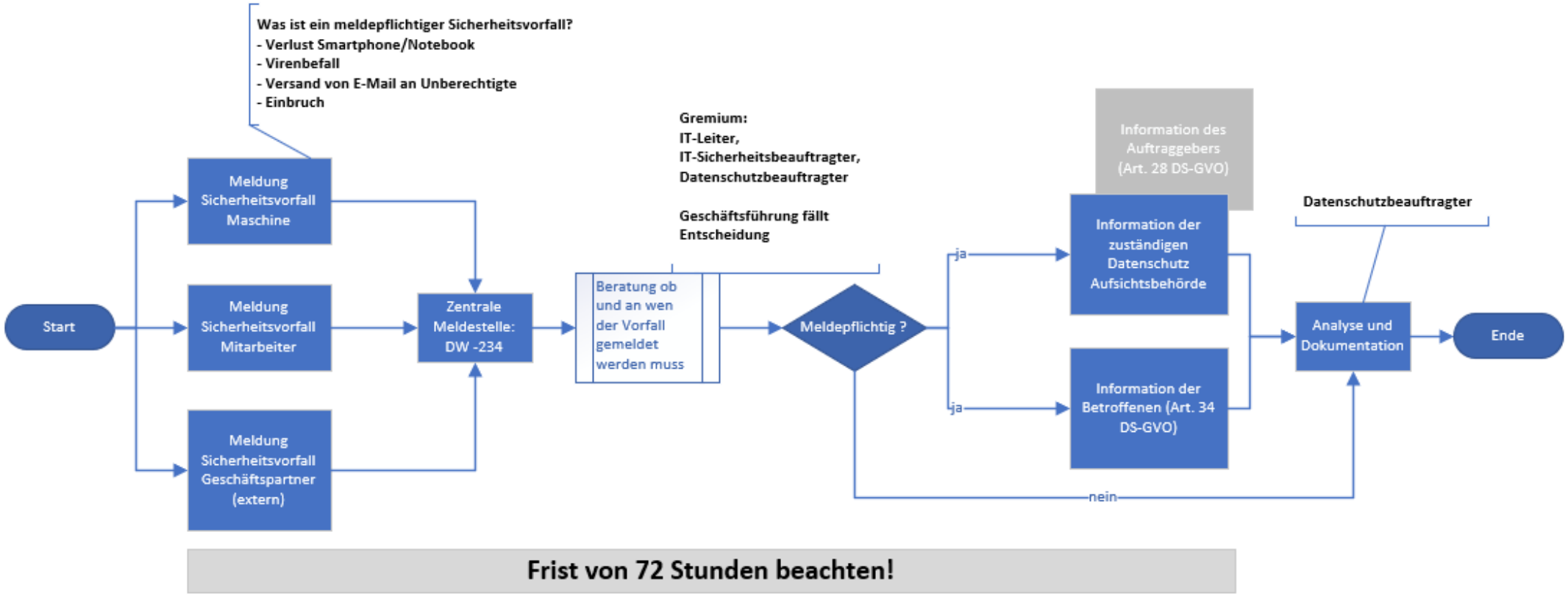
3 Vorgehen in der Praxis

a. **Meldeprozess modellieren**
b. **Mitarbeiter informieren/sensibilisieren**
c. **Meldeformular bereithalten**
d. **Online-Meldung durchspielen**

BSP-SECURITY

3 Vorgehen in der Praxis – Meldeprozess modellieren

Muster GmbH
MA 6.1 Meldeprozess Artt. 33, 34 DS-GVO (vereinfachter Musterprozess)
Autor: Michael Gruber (EDSB)
Letzte Änderung: 20.08.2018
Klassifikation: intern



BSP-SECURITY

we make security simple.

3 Vorgehen in der Praxis

Mitarbeiter informieren/sensibilisieren:

- **Schulung**
- **Newsletter**
- **Übungen**
- **…**

BSP-SECURITY

3 Vorgehen in der Praxis - Meldeformular

Mitteilung über Data-Breach / Datenpanne
- Vertraulich / Confidential

Wenn **personenbezogene Daten** unbeabsichtigt oder unrechtmäßig vernichtet oder verändert wurden, von Unbefugten zur Kenntnis genommen wurden bzw. verarbeitet wurden, an Unbefugte übermittelt wurden oder wenn es zu einer **Verletzung der Datensicherheit** gekommen ist, ist der Sachverhalt **sofort** nach Bekanntwerden des Vorfalls an den Datenschutzbeauftragten zu **melden**.

Bitte sofort melden an:

Zentrale Meldestelle: Datenschutzbeauftragten

Eventuell fehlende Informationen können nachgeliefert werden.

Vom Fachbereich bzw. Datenschutz-Koordinator auszufüllen	
Meldende Stelle (Kontaktdaten / Fachbereich)	Name: Fachbereich: Firma: (bei Auftragsverarbeitung) E-Mail: Telefon:
Wann wurde der Vorfall bekannt?	Datum: Uhrzeit:
Art des Vorfalls	**Verlust / Diebstahl Endgerät** ☐ Mobile, ungesicherte Datenträger (z.B. USB-Stick) ☐ Smartphone ☐ Tablet ☐ Notebook ☐ Desktop-PC Weitere: **Datenunzugänglichkeit** ☐ Datenverlust ☐ Unautorisierte Löschung ☐ Ransomware (verschlüsselt Daten gegen Lösegeld) Weitere: **Datendiebstahl** ☐ Hacking, Schadsoftware ☐ Einbruch Weitere: **Unautorisierte Weitergabe von Daten** ☐ Durch Dienstleister ☐ Durch Mitarbeiter ☐ Durch Systeme Weitere:
Sind die Daten / Datenträger verschlüsselt?	☐ Nein ☐ Ja ☐ Nicht bekannt Falls ja, welche Verschlüsselung:

Nähere Beschreibung	Wodurch wurde der Vorfall bekannt: Schilderung des Vorfalls:
Wo geschah der Vorfall?	☐ intern ☐ Externe Stelle, wo? ☐ Dienstleister Ansprechpartner: Mail: Telefon: Mobil: Adresse: ☐ Nicht bekannt
Wie viele Datensätze bzw. wie viele Personen sind von dem Vorfall betroffen?	**Datensätze** Anzahl (ggf. Schätzung) Ein **Datensatz** ist eine Gruppe von inhaltlich zusammenhängenden Datenfeldern, z. B. ‚Name', ‚Adresse' und ‚Geburtsdatum' bilden einen Datensatz zu einer Person. **Personen** Anzahl (ggf. Schätzung)
Betroffene Personengruppen	☐ Kunden ☐ Interessenten ☐ Berater ☐ Freie Mitarbeiter ☐ Azubis ☐ Mitarbeiter ☐ Bewerber ☐ Praktikanten ☐ Dienstleister (inkl. Ansprechpartner) ☐ Lieferanten (inkl. Ansprechpartner) ☐ User (auch Pseudonyme) ☐ Weitere
Betroffene Datenarten	☐ Kommunikations-/Kontaktdaten ☐ E-Mail Adresse ☐ Log-In Daten (Anmeldename, Passwörter, etc.) ☐ Bestellinformationen (Kaufhistorie, Rechnungsdaten, etc.) ☐ Bank- & Kreditkartendaten ☐ Nutzungsdaten (Einzelverbindungsnachweise, IP-Adressen, Logging, Registrierung, Anmeldung, etc.) ☐ Beschäftigtendaten (Gehalt, Sozialversicherung, bAV, etc.) ☐ Leistungsdaten (Mitarbeiterbewertung, etc.) ☐ Bild- und Videodaten ☐ Besondere personenbezogene Daten (Art. 9 Abs.1 DSGVO) Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Uberzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. ☐ Weitere Datenarten:
Betroffene Systeme (Name, Beschreibung)	☐ Nicht bekannt Z.B. Exchange, Webshop
Unterliegen die betroffenen Daten einem Berufsgeheimnis? (Betriebsarzt, Betriebsrat, etc.)	☐ Nein ☐ Ja ☐ Nicht bekannt Falls ja, welcher Art:
Welche Folgen der Datenschutzverletzung sind für die Betroffenen zu erwarten?	☐ Finanzieller Schaden ☐ Imageschaden ☐ Lebens- & Existenzgefährdung

BSP-SECURITY

we make security simple.

3 Vorgehen in der Praxis

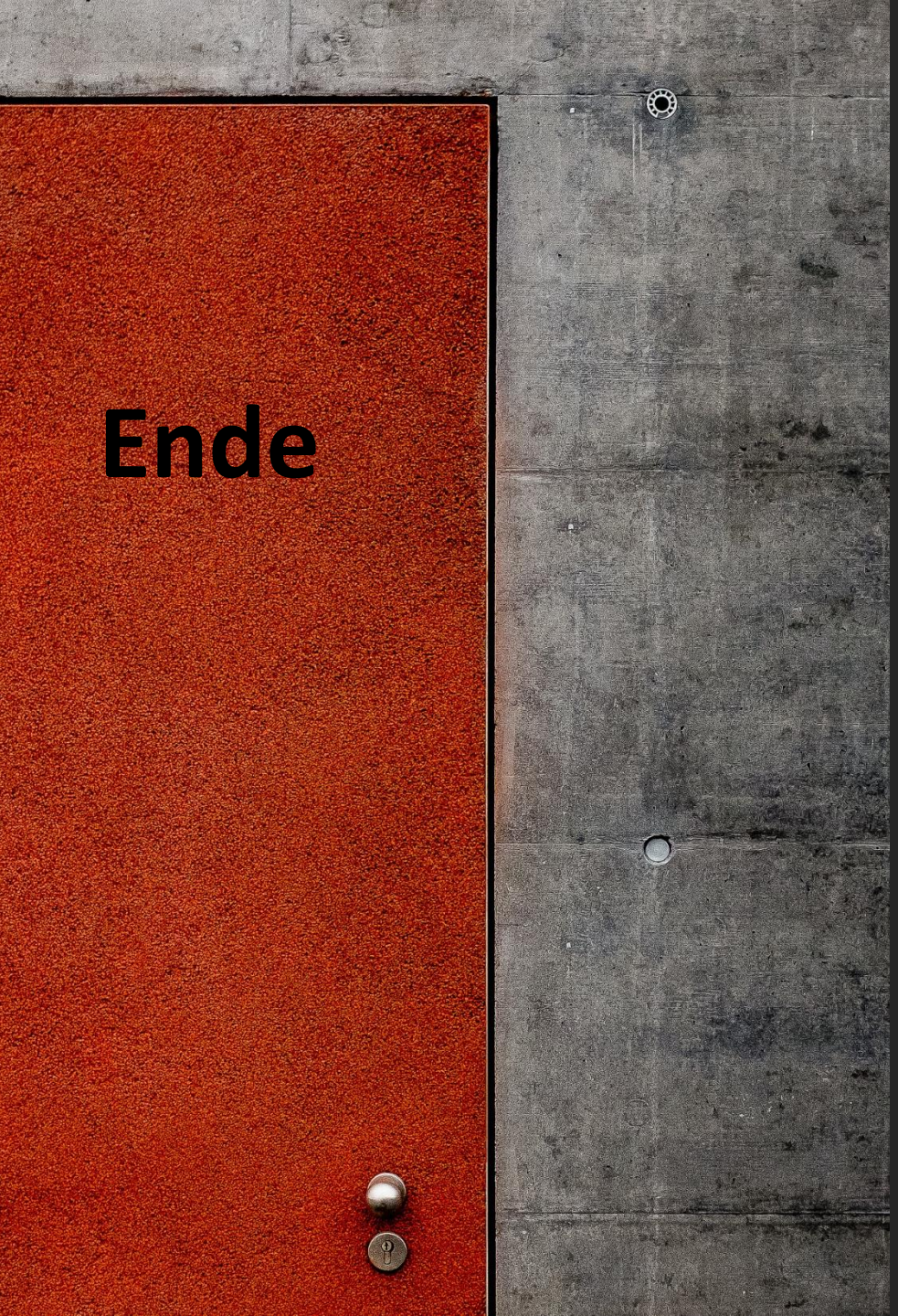
Prozess inkl. Online-Meldung durchspielen

Art. 83 Abs. 5 DS-GVO regelt Sanktionen bei Missachtung der Artt. 33, 34

10.000.000 € Geldbuße oder 2 % des weltweiten Jahres Umsatzes des gesamten Unternehmens

Und dieser Meldeprozess schützt auch die nicht personenbezogenen Daten (Kronjuwelen)

BSP-SECURITY



BSP-SECURITY

Michael Gruber

Senior Consultant Datenschutz und Informationssicherheit

ISIS12 Netzwerkpartner
Fachbeirat Bayerischer IT-Security Cluster e.V.

T +49 (0)941 46 29 09 29
M +49 (0)152 32 01 04 95

BSP-SECURITY
Franz-Mayer-Str. 1
D-93053 Regensburg

E-Mail: michael.gruber@bsp-security.de
www.bsp-security.de