|  |  |
| --- | --- |
| Vorgehensweise bei DatenschutzpanneVorlage:Formular zur Meldung bei Behörde/DSBArbeitshinweis:1. Sobald eine Datenschutzpanne (Data Breach) auftritt muss der Verantwortliche und der DSB informiert werden. Die Dokumentation des Falls wird mit Hilfe dieses Formulars durchgeführt.
 |    |

  **Dokumentation zur Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DSGVO**

**I Allgemeine und technische Angaben zum Vorfall**

1. **Allgemeine Angaben zum Vorfall**

Feststellung des Vorfalls:

Datum: Uhrzeit:

Zeitpunkt des Vorfalls, betroffener Zeitraum:

Datenverarbeitungsverfahren:

Verantwortlicher Fachbereich:

Verantwortlicher Bearbeiter für den Vorfall:

1. **Beschreibung der Datenpanne**

|  |
| --- |
| Betroffene Systeme/Objekte |
| Wie hat sich der Vorfall ereignet? |
| Welche Folgen wurden festgestellt? |

1. **Detailinformationen zur Datenpanne**

Letzte störungsfreie Nutzung:

Art der Nutzung:

Reaktionen und Zustand des Systems

|  |
| --- |
| Reaktionen/Maßnahmen auf die Datenpanne |
| Aktueller Zustand des Systems |

1. **Ursache der Datenpanne und Schwachstelle**

 Fehlerart

[ ]  Systemausfall

 [ ]  softwarebedingt

 [ ]  hardwarebedingt

[ ]  Wartungsfehler

 [ ]  Softwarewartung

 [ ]  Hardwarewartung

[ ]  Fehlbedienung

[ ]  Unbefugte Verwendung oder Verarbeitung der Daten

[ ]  Externe Ursachen (z. B. Hacking, Diebstahl, Sabotage), ggf. welche?

[ ]  Sonstige/andere Ursachen, ggf. welche?

 [ ]  Ursache unbekannt

**II Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DS-GVO**

1. Sind personenbezogene Daten betroffen?

 [ ]  Ja [ ]  Nein

1. Benachrichtigung des Datenschutzbeauftragten erledigt.

 Datum: Uhrzeit:

 [ ]  Entfällt (keine personenbezogenen Daten betroffen)

**Fortsetzung, wenn personenbezogene Daten betroffen sind**

1. **Angaben zum Vorfall**
	1. Art des Vorfalls:

(Vorfälle sind z. B. Verlust der Vertraulichkeit, Datendiebstahl, Zerstörung oder Verfälschung der Daten, Übermittlung an unbefugte Stellen etc.)

* 1. Betroffene Personengruppen:

(Hier ist insbesondere auch auf besonders schutzbedürftige Personengruppen wie Kinder, Behinderte u. a. zu achten.)

* 1. Zahl der betroffenen Personen:
	2. Kategorien von personenbezogenen Daten:

(Hier sind insbesondere besondere Datenarten i. S. v. Art. 9 DSGVO und sonstige sensible Daten wie Bankdaten, Passwörter etc. anzugeben.)

* 1. Wahrscheinliche Folgen/Risiken der Verletzung des Schutzes personenbezogener Daten

(Hier sind die möglichen Risiken und Folgen für die Betroffenen anzugeben. Vgl. Checkliste zur Risiko- und Schutzbedarfsermittlung.)

1. **Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten**
	1. Eingerichtete Maßnahmen

(Hier sind die Maßnahmen zu beschreiben, die zum Schutz der personenbezogenen Daten gegen Vorfälle dieser Art eingerichtet worden sind.)

* 1. Weitere beabsichtigte Maßnahmen

(Hier sind die Maßnahmen zu beschreiben, deren Einrichtung aufgrund des Vorfalls zusätzlich noch geplant sind.)

* 1. Maßnahmen zur Abmilderung möglicher nachteiliger Folgen

(Hier sind die Maßnahmen zu beschreiben, die zur Minderung von Schäden bzw. von nachteiligen Folgen für die Betroffenen eingerichtet bzw. getroffen worden sind, z.B. Information der Betroffenen mit Hinweisen zum Schutz vor oder Minderung von Schäden.)

1. **Risiko für die persönlichen Rechte und Freiheiten der Betroffenen**

(Die Risikoabwägung ist zu begründen bzw. das Ergebnis der Risiko- und Schutzbedarfsermittlung zugrunde zu legen.)

 [ ]  Geringes Risiko

 [ ]  Risiko i. S. v. Art. 33 DSGVO (mittleres Risiko)

 [ ]  Hohes Risiko i. S. v. Art. 34 DSGVO

1. **Meldungen und Benachrichtigungen**
	1. Meldung an die Aufsichtsbehörde für den Datenschutz

 Meldepflicht an die Aufsichtsbehörde [ ]  Ja [ ]  Nein

 Meldung (binnen 72 Stunden nach Feststellung des Vorfalls)

 Datum: Uhrzeit:

 Art der Meldung [ ]  Schriftlich per Post [ ]  Online [ ]  Sonstiges, Art:

 *https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/*

* 1. Benachrichtigung der Betroffenen
		1. Sind technische und organisatorische Maßnahmen getroffen, um die von der Schutzverletzung betroffenen Daten für Unbefugte unzugänglich zu machen, z. B. Verschlüsselung?

 [ ]  Ja [ ]  Nein

 Art der Maßnahmen:

(Hier sind Maßnahmen i. S. v. Art. 34 Abs. 3 lit. a DSGVO zu beschreiben, die einen unbefugten Zugang zu den von der Datenschutzverletzung betroffenen Daten und damit Schäden für die Betroffenen verhindern.)

* + 1. Ist durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach nicht mehr besteht?

 [ ]  Ja [ ]  Nein

Art der Maßnahmen:

(Hier sind nach dem Vorfall eventuell eingerichtete nachfolgende Maßnahmen i. S. v. Art. 34 Abs. 3 lit. b DSGVO zu beschreiben, die sicherstellen, dass das hohe Risiko für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach nicht mehr besteht.)

Welche Risiken sind durch die Maßnahmen nach Ziff. 4.2.1 und 4.2.2 beseitigt bzw. reduziert worden und inwieweit?

Art der Risiken:

(Hier sind die Risiken zu beschreiben, die durch die o. g. Maßnahmen konkret reduziert bzw. beseitigt worden sind.)

* + 1. Verbleibende Restrisiken

(Hier sind die nach Einführung der o. g. zusätzlichen Maßnahmen verbleibenden Restrisiken zu beschreiben und anschließend nach ihrer Risikostufe zu beurteilen.)

Ausmaß des Restrisikos

Risikostufe: [ ]  Gering [ ]  Mittel [ ]  Hoch

* + 1. Benachrichtigungspflicht der Betroffenen:

[ ]  Ja Datum der Benachrichtigung:

Art der Benachrichtigung

☐ Schriftlich per Post

[ ]  Sonstiges, Art:

Informationen, Maßnahmen und Empfehlungen an die Betroffenen:

(Hier ist zu beschreiben, welche Maßnahmen den Betroffenen zum Schutz ihrer Rechte und Freiheiten gegeben worden sind.)

[ ]  Keine Benachrichtigungspflicht (Art. 34 Abs. 3 DSGVO)

[ ]  Geeignete technische und organisatorische Maßnahmen getroffen

[ ]  Ein hohes Risiko besteht nicht mehr

[ ]  Benachrichtigung verursacht einen unverhältnismäßig hohen Aufwand

[ ]  Anstelle der Benachrichtigung öffentliche Bekanntmachung

* 1. Bei Auftragsverarbeitern Meldung an den Auftraggeber

[ ]  Ja [ ]  Nein

1. **Sonstige Maßnahmen**

Abstimmung mit der Aufsichtsbehörde für den Datenschutz, Anordnungen oder Maßnahmen

(Die Aufsichtsbehörde kann, soweit dies noch nicht geschehen ist, die Benachrichtigung der Betroffenen verlangen oder feststellen, dass eine Ausnahme von der Benachrichtigungspflicht vorliegt. Hier werden evtl. Anordnungen oder Feststellungen der Aufsichtsbehörde dokumentiert.)

Anzeige bei Strafverfolgungsbehörden

[ ]  Ja [ ]  Nein

Verfahrensverantwortlicher:

Ort, Datum: Unterschrift:

Datenschutzbeauftragter:

Ort, Datum: Unterschrift: