Datenschutzbehörde

Felder zur Meldung von Datenschutzverletzungen TEIL 2

Inhalt

1. Informationen

Informationen zur Verarbeitung personenbezogener Daten

Die Datenschutzbehörde verarbeitet Ihre personenbezogenen Daten, weil sie gesetzlich verpflichtet ist, Datenschutzverletzungen zu registrieren, deren Einhaltung zu überwachen und durchzusetzen sowie die betroffene Organisation bei Bedarf zu beraten. Die personenbezogenen Daten werden so lange gespeichert, wie dies im Rahmen von Beratung, Überwachung und Durchsetzung erforderlich ist, und zwar bis zu zehn Jahre nach Abschluss des Dossiers (bei einem Rechtsverfahren bis zum Ende des Verfahrens). Im Rahmen der Zusammenarbeit mit anderen europäischen und/oder nationalen Datenschutzbehörden können Daten aus diesem Formular an diese weitergegeben werden.

Weitere Informationen oder Hinweise zur Ausübung Ihrer Datenschutzrechte finden Sie in unserer Datenschutzerklärung.

Dieses Meldeformular dient der Meldung einer Datenschutzverletzung an die Datenschutzbehörde gemäß Artikel 33 DSGVO.

Handelt es sich um eine Datenschutzverletzung, die ebenfalls in den Anwendungsbereich des Gesetzes über elektronische Kommunikation fällt, und handelt es sich bei dem Verantwortlichen um einen Betreiber elektronischer Kommunikationsdienste, der beim BIPT gemeldet ist, wird eine Kopie dieser Meldung gemäß Art. 107/3, §2 WEC an das BIPT weitergeleitet.

Der Verantwortliche informiert die Datenschutzbehörde spätestens 72 Stunden nach Kenntnisnahme über eine Datenschutzverletzung.

Felder für freien Text weisen eine maximale Länge von 100 Zeichen (einschließlich Leerzeichen) auf, sofern nicht anders angegeben.

Um die Datenschutzverletzung problemlos zu melden, benötigen Sie (möglicherweise) die folgenden Informationen für den Meldeprozess.

- Falls zutreffend: Kontaktdaten und Referenz des aktiven DPO-case der Meldung Ihres DPOs

- Korrespondenz über die Feststellung der Datenschutzverletzung
- Falls zutreffend: Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO)
- Verzeichnis der Datenschutzverletzungen (Artikel 33.5 DSGVO)
- Bereits vor der Datenschutzverletzung geltende Maßnahmen
- Maßnahmen, die ergriffen wurden, um die Datenschutzverletzung zu beenden
- Maßnahmen, die ergriffen wurden oder vorgesehen sind, um die Datenschutzverletzung in Zukunft zu verhindern
- Gegebenenfalls: Stellungnahme des DPOs
- Datenschutz-Folgenabschätzung (DSFA) (Art. 35 DSGVO) (falls zutreffend)
- Falls zutreffend: Benachrichtigung des von einer Verletzung des Schutzes personenbezogener Daten Betroffenen (Art. 34 DSGVO)

Wenn es sich um Hacking (im weitesten Sinne), Phishing oder einen anderen (Cyber-)Vorfall handelt, bei dem eine (externe) Untersuchung stattgefunden hat:

- Untersuchungsbericht zu der Datenschutzverletzung

Wenn Sie mit einem Auftragsverarbeiter zusammenarbeiten oder die Datenschutzverletzung bei einem Dritten stattgefunden hat:

- Auftragsverarbeiter (Art. 28 DSGVO)
- Protokollvereinbarungen zwischen Behörden (Art. 20 Rahmengesetz)
- Andere Vereinbarungen, wie z. B. eine Kooperationsvereinbarung (Art. 26 DSGVO – gemeinsam Verantwortliche)

Wenn Sie ein nicht in der Union ansässiger Verantwortlicher oder Auftragsverarbeiter sind:

- Vertretervereinbarung (Art. 27 DSGVO)

Untersuchung bei *Hacking* (im weitesten Sinne), *Phishing* oder einem anderen Cyber-Vorfall, bei dem personenbezogene Daten betroffen waren

Wenn Sie der Datenschutzbehörde eine Datenschutzverletzung aufgrund von *Hacking* (im weitesten Sinne), *Phishing* oder einem anderen (Cyber-)Vorfall melden, bei dem personenbezogene Daten betroffen waren, gehen wir davon aus, dass Sie so schnell wie möglich eine Untersuchung zum Umfang des Vorfalls durchführen oder durchführen lassen. Diese Untersuchung ist notwendig, um sicherzustellen, dass:

- Keine *Backdoors* und andere schädliche Dateien im System verbleiben
- Klarheit darüber gewonnen wird, ob personenbezogene Daten von Dritten eingesehen, kopiert, gestohlen oder verändert wurden.

Die Datenschutzbehörde geht davon aus, dass Sie folgende Fragen in Ihre Untersuchung einbeziehen:

- Bestand Zugriff auf personenbezogene Daten, z. B. auf E-Mails in einem E-Mail-Postfach, auf Druckaufträge auf einem *Printserver*, auf den Inhalt einer Datenbank, auf Dateien auf einem *Fileserver*, auf dem personenbezogene Daten verarbeitet werden usw.?
- Wurden diese personenbezogenen Daten kopiert, eingesehen oder auf andere Weise an die Hacker gesendet? Wurde ein *Flow* (über die Firewall oder anderweitig) zu einer Umgebung außerhalb des Unternehmens festgestellt?

- Sind Logdaten verfügbar, und falls ja, ist es möglich, anhand dieser Logdaten auszuschließen, dass personenbezogene Daten kopiert oder eingesehen wurden?

Dokumentationspflicht – Verzeichnis der Datenschutzverletzungen:

Die Meldung einer Datenschutzverletzung an die Datenschutzbehörde, sofern dadurch ein mögliches Risiko für die Rechte und Freiheiten natürlicher Personen besteht, gehört zu den Pflichten im Zusammenhang mit Datenschutzverletzungen. Die Verantwortlichen sind ebenfalls verpflichtet, diese intern im Verzeichnis der Datenschutzverletzungen zu erfassen. Diese Dokumentationspflicht gilt im Übrigen für alle Datenschutzverletzungen, also auch für solche, die kein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Gemäß Art. 33.5 DSGVO müssen mindestens folgende Informationen enthalten sein:

- Fakten zu der Datenschutzverletzung, wie z. B. die Ursache, was genau passiert ist, wann genau welche Maßnahmen ergriffen wurden und um welche personenbezogenen Daten es sich handelt
- Folgen der Datenschutzverletzung
- Maßnahmen, die ergriffen wurden, um die Datenschutzverletzung zu beenden und eine Wiederholung zu verhindern

Meldung einer Datenschutzverletzung, bei der unterschiedliche Risikostufen für verschiedene Betroffene bestehen

Wenn Sie eine Datenschutzverletzung melden, die unterschiedliche Risikostufen für verschiedene Betroffene aufgrund desselben Vorfalls zur Folge hat, müssen Sie in Ihrer Meldung die höchsten Risikostufen angeben.

2. Einführung

Auf der Grundlage welcher Vorschriften melden Sie?*

☐ Allgemeine Datenschutzverordnung (AVG) – Art. 33 AVG
☐ Gesetz über elektronische Kommunikation (WEC) – Art 107/3, §3 WEC
☐ Wirtschaftsgesetzbuch (WER) – Art. XII.27 WER

Wenn Sie unter die NIS(II) fallen, müssen Sie zusätzlich eine Meldung beim CCB über den folgenden Link vornehmen: https://notif.safeonweb.be/de

Wenn Sie ein Finanzdienstleister sind, müssen Sie möglicherweise zusätzlich eine Meldung bei der NBB unter PSDII über den folgenden Link vornehmen: https://www.nbb.be/en/onegate

2.1. Haben Sie die Datenschutzverletzung auch anderen nationalen Aufsichtsbehörden aufgrund anderer Meldepflichten gemeldet oder eine Beschwerde bei der Polizei und/oder der Staatsanwaltschaft eingereicht? Oder werden Sie dies noch tun und bei welcher Behörde?

Dropdown:
Ja (go to 2.1.1.)
Nein

2.1.1. Liste der Aufsichtsbehörden

☐ Centrum voor Cybersecurity België (Zentrum für Cybersicherheit Belgien) CCB – Cyber Emergency Response Team (Cyber-Notfallteam) CERT

*Ref. CCB**

☐ Nationale Bank van België (Nationale Bank von Belgien) NBB

*Ref. BNB**

☐ FÖD Wirtschaft

*Ref. FÖD Wirtschaft**

☐ Belgisch Instituut voor Postdiensten en Telecommunicatie (Belgisches Institut für Postdienste und Telekommunikation (BIPT)

*Ref. BIPT**

☐ (Lokale oder föderale) Polizei und/oder Staatsanwaltschaft

*Protokollnummer (PV-Nummer)**

☐ Andere Aufsichtsbehörde

*Andere Aufsichtsbehörde**	*Referenz andere Aufsichtsbehörde**

3. Organisation

3.1. Kontaktdaten des Verantwortlichen

3.2. Name der Organisation*

Feld für freien Text

3.3. Hauptsitz*

- ○ In Belgien (go to 3.3.1.)
- ○ In einem EU-/EWR-Land (go to 3.3.2 und 3.3.3.)
- ○ Außerhalb der EU/des EWR (go to 3.3.2 und 3.3.4.)

3.3.1. Unternehmensnummer*

Bereits auf Grundlage des Anmeldeablaufs oder auf Grundlage des Unternehmenskontos ausgefüllt

3.3.2. Land des Hauptsitzes*

Dropdown-Menü: Länderliste – eine Auswahl möglich

3.3.3. Europäische Umsatzsteuer-Identifikationsnummer*

Strukturiertes Textfeld

3.3.4. Eindeutiger Ländercode*

Feld für freien Text

3.4. In welcher Branche ist der Verantwortliche tätig?*

Dropdown-Auswahlliste Branche – mehrere Antworten möglich:
Verwaltungs- und Unterstützungsdienste
Sonstige (go to 3.4.1.)

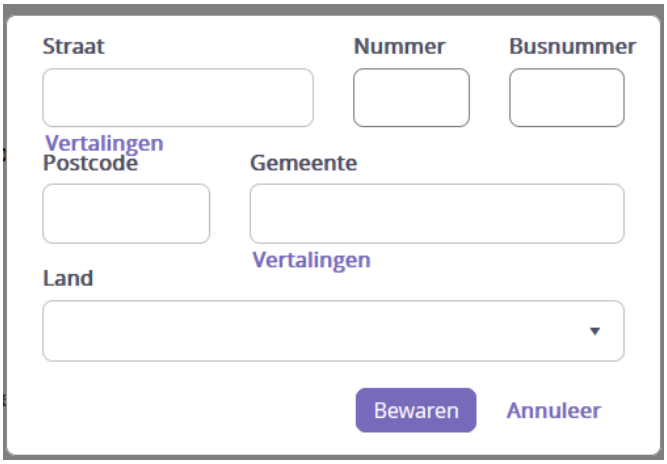
Arbeit(svermittlung), Zeitarbeitsagenturen und Personalverwaltung
Baugewerbe
Grundstücks- und Wohnungswesen
Exterritoriale Organisationen und Körperschaften
Finanzielle Aktivitäten und Versicherungen
Groß- und Einzelhandel
Gastgewerbe
Industrie
Information und Kommunikation
Kunst, Kultur, Unterhaltung und Erholung
Gesundheits- und Sozialwesen
Versorgungsunternehmen
Bildung
Öffentliche Verwaltung
Sonstige Dienstleistungen
Sonstige Organisationen – Weltanschauliche Organisationen
Sonstige Organisationen – politische Organisationen
Sonstige Organisationen – Gewerkschaften
Sonstige unternehmensbezogene Dienstleistungen – Wirtschaftsprüfung, Steuerberatung und Verwaltung
Sonstige unternehmensbezogene Dienstleistungen – wissenschaftliche Forschung
Polizei und Justiz
Soziale Netzwerke (Unternehmen)
Verkehr
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen

3.4.1. Sonstige Branchen*

Feld für freien Text

3.5. Adressdaten und Kontaktdaten des Verantwortlichen* (?)

(?) Benötigen Sie Hilfe? Informationsadresse: Es werden automatisch nur belgische Adressen ausgefüllt. Andere Adressen können problemlos manuell eingegeben werden, wobei die vorgeschlagene Adresse ignoriert oder überschrieben werden kann.



3.6. E-Mail-Adresse des Verantwortlichen* (?)

(?) Benötigen Sie Hilfe? E-Mail-Adresse des Verantwortlichen: Bitte geben Sie hier eine allgemeine E-Mail-Adresse für das Unternehmen und keine persönliche E-Mail-Adresse oder eine E-Mail-Adresse ein, die direkt identifizierbare personenbezogene Daten enthält.

Feld für freien Text

3.7. Ist der Verantwortliche ein (Telekommunikations-)Betreiber, der beim BIPT registriert ist?* (?)

(?) Benötigen Sie Hilfe? BIPT: https://www.bipt.be/operatoren/publication/lijst-van-telecomoperatoren

Dropdown:
Ja
Nein

3.8. Ist der Verantwortliche ein börsennotiertes Unternehmen?*

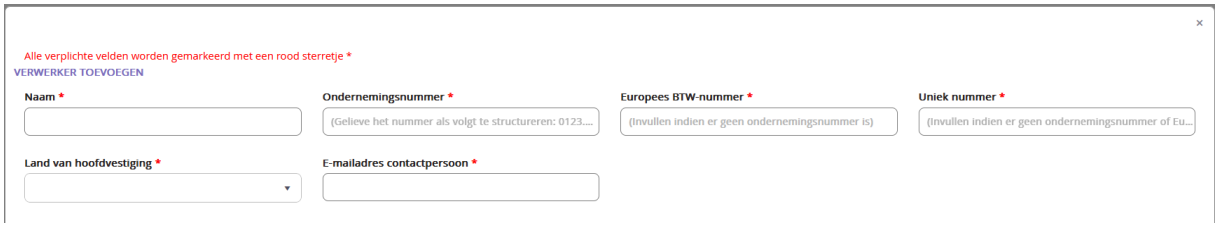
Dropdown:
Ja
Nein

3.9. Hat die Datenschutzverletzung bei einer Verarbeitung stattgefunden, die an einen Auftragsverarbeiter ausgelagert wurde?*

Dropdown:
Ja (go to 2.9.1.)
Nein

3.9.1. Um welchen Auftragsverarbeiter handelt es sich?*

Hinzufügen: (mehrere Angaben möglich)



3.10. Kontaktperson für die Datenschutzverletzung

Name der Person*

Feld für freien Text

Vorname der Person*

Feld für freien Text

Funktion der Kontaktperson

Feld für freien Text

Telefonnummer der Kontaktperson*

Strukturiertes Textfeld

E-Mail-Adresse der Kontaktperson*

Strukturiertes Textfeld

3.11. Verfügt der Verantwortliche über einen DPO?*

Dropdown:
Ja (go to 3.11.1)
Nein

3.11.1. DPO-case*

Auswählen

Wenn Sie Ihren DPO noch nicht angemeldet haben, melden Sie ihn bitte zunächst über das Portal an

4. International

4.1. Grenzüberschreitende Datenschutzverletzung

4.1.1. Hat die Datenschutzverletzung Auswirkungen auf Betroffene in mehreren Ländern?*

Dropdown:
Ja (go to 4.1.2 und 4.2.1.)
Nein

4.1.2. Wenn es sich um eine grenzüberschreitende Verarbeitung handelt, um welche Länder (einschließlich Belgien, falls zutreffend) handelt es sich und wie viele Betroffene gibt es in diesen Ländern (?)*

(?) Benötigen Sie Hilfe? Bitte geben Sie unten die verschiedenen Länder und die Anzahl der Personen für diese Länder an, die von der grenzüberschreitenden Datenschutzverletzung betroffen sind. Falls es nicht möglich ist, die genaue Anzahl der Personen zu ermitteln, geben Sie bitte eine ungefähre Zahl an.

Hinzufügen: (mehrere Angaben möglich)

Land	Betroffene
Auswahlliste Länder	*Anzahl der Betroffenen*

4.1.3. Befindet sich der Hauptsitz oder der einzige Sitz des Verantwortlichen in Belgien?*

Dropdown:
Ja
Nein

4.1.4. Erfolgt die Meldung auf der Grundlage des One-Stop-Shop-Verfahrens?*(?)

(?) Benötigen Sie Hilfe? One-Stop-Shop-Verfahren: Das One-Stop-Shop-Verfahren ist ein Mechanismus, bei dem eine Aufsichtsbehörde als federführende Aufsichtsbehörde für Verantwortliche mit mehreren Niederlassungen im Europäischen Wirtschaftsraum fungiert. In diesem Fall ist die federführende Aufsichtsbehörde die Aufsichtsbehörde des Mitgliedstaats, in dem sich der Hauptsitz des Verantwortlichen befindet. Bei der Meldung von Datenschutzverletzungen mit grenzüberschreitenden Auswirkungen kann ein Verantwortlicher mit mehreren Niederlassungen im EWR das One-Stop-Shop-Verfahren nutzen, indem er die Datenschutzverletzung (ausschließlich) der Aufsichtsbehörde meldet, in deren Zuständigkeitsbereich sich sein Hauptsitz befindet.

Dropdown:
Ja
Nein

4.2. Zuständige Aufsichtsbehörden in anderen EU-Mitgliedstaaten

4.2.1. Hat Ihre Organisation die Datenschutzverletzung anderen Datenschutzbehörden gemeldet?*

Dropdown:
Ja (go to 4.2.1.1.)
Nein

4.2.1.1. Bitte geben Sie an, in welchen Ländern Sie die Datenschutzverletzung den Datenschutzbehörden gemeldet haben*

Hinzufügen: (mehrere Angaben möglich)

Auswahlliste Länder

4.2.2. Wird die Datenschutzverletzung noch anderen Datenschutzbehörden gemeldet?*

Dropdown:

Ja (go to 4.2.2.1.)
Nein

4.2.2.1. Bitte geben Sie an, in welchen Ländern Sie die Datenschutzverletzung noch den Datenschutzbehörden melden werden*

Hinzufügen: (mehrere Angaben möglich)

Auswahlliste Länder

5. Zeitleiste

5.1. Datum und Uhrzeit, zu denen die Datenschutzverletzung stattgefunden hat*

Wann hat die Datenschutzverletzung stattgefunden?*

Dropdown:
Nicht bekannt
Das genaue Datum und die Uhrzeit, zu denen die Datenschutzverletzung stattfand, sind bekannt, nämlich (go to 5.1.1.)
Das genaue Datum und die Uhrzeit, zu denen die Datenschutzverletzung stattfand, sind nicht bekannt, werden jedoch wie folgt geschätzt: (go to 5.1.1.)

5.1.1. Datum und Uhrzeit, zu denen die Datenschutzverletzung stattgefunden hat*

Datumsfeld: Kalender	*Zeitfeld: Uhrzeit*

5.2. Datum und Uhrzeit, zu denen die Datenschutzverletzung festgestellt wurde*

Wann wurde die Datenschutzverletzung festgestellt?*(?)

(?) Benötigen Sie Hilfe? Datenschutzverletzung – Datum und Uhrzeit der Feststellung der Datenschutzverletzung: Der Zeitpunkt der Feststellung einer Datenschutzverletzung ist nicht identisch mit dem Zeitpunkt, zu dem der Vorfall dem DPO gemeldet wird. Der DPO ist nicht für die Meldepflicht gegenüber einer Aufsichtsbehörde verantwortlich. Die Datenschutzbehörde akzeptiert daher den Zeitpunkt der Meldung an den DPO nicht als Rechtfertigung für eine verspätete Meldung.

Datumsfeld: Kalender (go to 5.4, falls zutreffend)	*Zeitfeld: Uhrzeit (go to 5.4, falls zutreffend)*

5.3. Art der Feststellung der Datenschutzverletzung*

Dropdown:
Interne Meldung (go to 5.3.1.)
Externe Meldung (go to 5.3.2.)

5.3.1. Interne Meldung

Auswahlliste: mehrere Antworten möglich

☐ Verlust von Hardware

- ☐ Verwaltungsprozess (z. B. IT-Vorfallmeldesystem, Informationssicherheits-Vorfallmanagement usw.)
- ☐ Verfahren des Cyber-Notfallteams
- ☐ Kontrollsystem zur Erkennung von Eindringversuchen oder Sicherheitsverletzungen und zur Aufdeckung unbefugter Zugriffe
- ☐ Kontrollverfahren/Whistleblower-Regelung
- ☐ Dienst für Beschwerdebearbeitung
- ☐ Sonstige: *(Feld für freien Text: bitte Name und Uhrzeit angeben*)*

5.3.2. Externe Meldung

Auswahlliste: mehrere Antworten möglich

- ☐ Durch einen Lieferanten, Subunternehmer oder Verarbeiter (go to 5.3.2.1.)
- ☐ Durch einen Kunden (go to 5.3.2.1.)
- ☐ Durch einen Dritten (go to 5.3.2.1.)
- ☐ Durch einen ethischen Hacker
- ☐ Durch eine Behörde (go to 5.3.2.1.)

5.3.2.1. Bei externer Meldung durch einen Lieferanten, Subunternehmer, Verarbeiter, Kunden, Dritten oder eine Behörde*

Feld für freien Text: Bitte Namen und Zeitpunkt angeben

5.4. Rechtfertigung für die verspätete Meldung der Datenschutzverletzung an die Datenschutzbehörde*

Wenn diese Meldung nicht innerhalb von 72 Stunden nach Feststellung der Datenschutzverletzung erfolgt: was ist der Grund dafür? Feld für freien Text – (DSGVO)
Wenn diese Meldung nicht innerhalb von 24 Stunden nach Feststellung der Datenschutzverletzung erfolgt: was ist der Grund dafür? Feld für freien Text – (WEC /WER)

5.5. Wann wurde die Datenschutzverletzung behoben?*

Dropdown:
Die Datenschutzverletzung wurde noch nicht behoben (go to 5.4.1.)
Die Datenschutzverletzung wurde behoben (go to 5.4.2.)

5.5.1. Der Grund dafür ist:*

Feld für freien Text

5.5.2. Wann wurde die Datenschutzverletzung behoben?*

Datumsfeld: Kalender	*Zeitfeld: Uhrzeit*

6. Verarbeitung

6.1. Zwecke, für die die personenbezogenen Daten verarbeitet werden*

Feld für freien Text

6.2. Art der von der Datenschutzverletzung beeinträchtigten personenbezogenen Daten*

Personenbezogene Daten im Allgemeinen *(Auswahlliste: mehrere Antworten möglich)*

- ☐ Identifikationsdaten (z. B. Name, Adresse, Geburtsdatum, Telefonnummer, Kfz-Kennzeichen, Kundennummer usw.)
- ☐ Elektronische Identifikationsdaten (z. B. E-Mail-Adressen, IP-Adressen usw.)
- ☐ Persönliche Merkmale (z. B. Alter, Geschlecht, Familienstand usw.)
- ☐ Physische Merkmale (z. B. Größe, Gewicht, Aussehen usw.)
- ☐ Zusammensetzung der Familie
- ☐ Freizeitaktivitäten und Interessen
- ☐ Social-Media-Profil
- ☐ Mitgliedschaften
- ☐ CRM-Daten (z. B. Informationen über Kunden, Kontakte, Kommunikation, Zufriedenheit usw.)
- ☐ (Kunden-)Profile (z. B. Vorhersage eines bestimmten Merkmals oder Verhaltens usw.)
- ☐ Lebens-, Klick-, E-Mail-, Such-, Surf-, Zahlungs- und/oder Konsumgewohnheiten
- ☐ Produkte und Dienstleistungen (Kosten, Verbrauch, Wartung usw.)
- ☐ Wohnungs- und Fahrzeugmerkmale
- ☐ Fotos oder Bildaufnahmen (z. B. CCTV, Überwachungskamera, aufgezeichnete Schulung usw.)
- ☐ Tonaufnahmen (z. B. aufgezeichnete Telefongespräche aus Callcentern, Kundendienst usw.)
- ☐ Ausbildung und Weiterbildung
- ☐ Beruf und Beschäftigung, Mehrwertsteuerregelung
- ☐ HR-Daten (Daten zu Gehalt und Personalpräsenz, Bewertungen, KPI, Karriereplanung usw.)
- ☐ Physische und/oder IT-Sicherheitsdaten von Kunden, Personal und Besuchern (z. B. Zugangsberechtigungen und Rechte, Verwendung von Ausweisen, Internetzugang usw.)
- ☐ Daten zur Kontrolle von Kunden oder Personal (z. B. Protokollierung, Whistleblower-Regelung, Beschwerdebearbeitung, Qualitätskontrolle usw.)
- ☐ Sonstige: *(Feld für freien Text*)*

Eindeutige Identifikationsnummer *(Auswahlliste: mehrere Antworten möglich)*

- ☐ Nationale Nummer (z. B. nationale Personenkennnummer)
- ☐ Sozialversicherungsnummer
- ☐ Sonstige: *(Feld für freien Text*)*

Besondere Kategorien personenbezogener Daten (Artikel 9.1 DSGVO) *(Auswahlliste: mehrere Antworten möglich)*

- ☐ Rassische oder ethnische Herkunft
- ☐ Politische Meinungen
- ☐ Religiöse oder weltanschauliche Überzeugungen
- ☐ Gewerkschaftszugehörigkeit
- ☐ Genetische Daten (z. B. DNA, Blutgruppe usw.)
- ☐ Biometrische Daten (z. B. Fingerabdruck, Iris-Scan usw.)
- ☐ Gesundheitsdaten
    - ☐ Physische Daten
    - ☐ Psychische Daten
    - ☐ Daten im Zusammenhang mit der Gesundheitsversorgung
    - ☐ Sonstige: *(Feld für freien Text)*
- ☐ Daten zum Sexualleben oder der sexuellen Orientierung

Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Artikel 10 DSGVO)*(Auswahlliste: mehrere Antworten möglich)*

- ☐ Strafrechtliche Verurteilungen
- ☐ Straftaten
- ☐ Sicherheitsmaßnahmen im Zusammenhang mit strafrechtlichen Verurteilungen oder Straftaten
- ☐ Auszug aus dem Strafregister

Personenbezogene Daten außerhalb der Artikel 9.1 und 10 DSGVO, die als sensibel behandelt werden, da ihre Verarbeitung ein bestimmtes Risiko für die Rechte und Freiheiten der Betroffenen darstellen kann, wie z. B. (*Auswahlliste: mehrere Antworten möglich*)

- ☐ Inhalt elektronischer Kommunikationsdaten
- ☐ Smart Grid (z. B. intelligente Zähler usw.)
- ☐ Standortdaten im weiteren Sinne (z. B. verarbeitet oder nicht verarbeitet durch Telekommunikationsbetreiber oder über Navigationssoftware, GPS usw.)
- ☐ Finanzdaten (Bankkartennummer, Kontonummer, Versicherungsnummer, Gehalt und Einkommen usw.)
- ☐ Zugangscode (Passwort, PIN-Code usw.)
- ☐ Kopien von Reisepass, elektronischem Personalausweis oder anderen Ausweisdokumenten
- ☐ Sonstige: *(Feld für freien Text*)*

6.3. Anzahl der Betroffenen, deren personenbezogene Daten beeinträchtigt wurden*

6.3.1. Ist die genaue Anzahl der Betroffenen bekannt?*

Dropdown:
Ja (go to 6.3.1.1.)
Nein (go to 6.3.1.2.)

6.3.1.1. Anzahl der Personen/Betroffenen*

Anzahl/Zahl

6.3.1.2. Mindest-/Höchstanzahl der Personen/Betroffenen*

Von mindestens wie vielen Personen sind personenbezogene Daten von der Datenschutzverletzung beeinträchtigt (als Opfer)?	Von höchstens wie vielen Personen sind personenbezogene Daten von der Datenschutzverletzung beeinträchtigt (als Opfer)?
Anzahl/Zahl	*Anzahl/Zahl*

6.4. Von der Datenschutzverletzung beeinträchtigte Personengruppen*

Mehrere Antworten möglich

- ☐ Bürger
- ☐ Verbraucher
- ☐ Benutzer
- ☐ Häftlinge
- ☐ Lieferanten
- ☐ Kinder
- ☐ Soldaten oder Polizeibeamte
- ☐ Ältere Menschen

- ☐ Patienten
- ☐ Schüler und/oder Studenten
- ☐ Flüchtlinge und Asylsuchende
- ☐ Arbeitnehmer/Mitarbeiter (Bewerber)
- ☐ Sonstige *(Feld für freien Text: Sonstige, nämlich:*)*
- ☐ Nicht bekannt

6.5. Grad und Möglichkeit der Identifizierung der betroffenen Personen auf der Grundlage der zugrunde liegenden Daten* (?)

(?) Benötigen Sie Hilfe? Grad der Identifizierung des/der Betroffenen: Direkt identifizierbare Daten – Daten, aus denen die Identität der Betroffenen für Dritte unmittelbar ersichtlich ist.

Indirekt und leicht identifizierbare Daten – Daten, aus denen die Identität der Betroffenen nicht unmittelbar hervorgeht, die jedoch von Dritten relativ einfach mit (öffentlich) zugänglichen Identifikationsdaten verknüpft werden können.

Indirekt identifizierbare Daten – Daten, aus denen nicht alle Dritten die Identität des Betroffenen direkt ableiten können. Es existieren jedoch Methoden, mit denen die bürgerliche Identität des Betroffenen mithilfe zusätzlicher (nicht öffentlicher) Daten dennoch ermittelt werden kann.

Indirekt auf Betroffene zurückführbare Daten – Es existieren Techniken und Methoden, die es Dritten ermöglichen, (Teile) eines Datensatzes bestimmten Personen zuzuordnen (sogenanntes „Single Out" von Personen in Datensätzen).

Mehrere Antworten möglich

- ☐ Direkt identifizierbare Daten
- ☐ Indirekt und leicht identifizierbare Daten
- ☐ Indirekt identifizierbare Daten
- ☐ Indirekt auf Betroffene zurückführbare Daten

7. Ursache

7.1. Was ist die Ursache für die Datenschutzverletzung?

Die Ursache für die Datenschutzverletzung lag*

Dropdown:
Intern (z. B. durch Personal)
Extern (z. B. durch einen Hacker)

Die Datenschutzverletzung wurde verursacht durch*

Dropdown:
Systemtechnisches Handeln
Menschliches Handeln

Die Absicht hinter der Datenschutzverletzung war*

Dropdown:
Zufällig
Böswillig

7.2. Was ist die Art der Datenschutzverletzung?

- ☐ Verletzung der Vertraulichkeit personenbezogener Daten – Vertraulichkeitsverletzung (go to 7.2.1.)
- ☐ Verletzung der Verfügbarkeit personenbezogener Daten – Verfügbarkeitsverletzung (go to 7.2.2.)
- ☐ Verletzung der Integrität der personenbezogenen Daten – Integritätsverletzung (go to 7.2.3.)

7.2.1. Weiterleitung – Größenordnung der Datenempfänger* (?)

(?) Benötigen Sie Hilfe? Anzahl der Personen

- *Begrenzte Gruppe: Weniger als 10 % der Mitarbeiterzahl.*
- *Große Gruppe: Ab 10 % der Mitarbeiterzahl.*

Boolesche Auswahl: eine Option

- ○ Unbekannte Anzahl von Personen
- ○ Bekannte Anzahl von Personen:
  - ○ Eine Person oder Organisation
  - ○ Eine begrenzte Gruppe
  - ○ Eine große Gruppe

7.2.2. Die Daten sind* (?)

(?) Benötigen Sie Hilfe? Verfügbarkeit der Daten:

- *Langer Zeitraum: Bitte legen Sie dies selbst in Abhängigkeit von der Funktion und dem Kontext der Verarbeitungsaktivitäten fest.*
- *Kurzer Zeitraum: Bitte legen Sie dies selbst in Abhängigkeit von der Funktion und dem Kontext der Verarbeitungsaktivitäten fest.*

Boolesche Auswahl: eine Option

- ○ Definitiv nicht verfügbar
- ○ Vorübergehend nicht verfügbar:
  - ○ Für einen langen Zeitraum
  - ○ Für einen kurzen Zeitraum

7.2.3. Umfang der Auswirkungen*

- ○ Die Daten sind unzuverlässig, fehlerhaft und können nicht mehr geändert, wiederhergestellt oder repariert werden.
- ○ Änderungen an den Daten können anhand von Protokollen und/oder Backups wiedergefunden, wiederhergestellt oder repariert werden.

7.3. Art der Datenschutzverletzung * (?)

(?) Benötigen Sie Hilfe? Art der Datenschutzverletzung Weitere Informationen zu den verschiedenen Arten von Datenschutzverletzungen in diesem Formular finden Sie in

unserer Benutzeranleitung zu Datenschutzverletzungen auf der Website der Datenschutzbehörde.

Mehrere Antworten möglich

- ☐ E-Mail mit personenbezogenen Daten an falsche Empfänger gesendet (go to 7.3.1.)
- ☐ E-Mail mit personenbezogenen Daten an Empfänger im Feld „An“ oder „Cc“ statt „Bcc“ gesendet (go to 7.3.2.)
- ☐ Brief oder Paket mit personenbezogenen Daten an den falschen Empfänger gesendet oder zugestellt (go to 7.3.3.)
- ☐ Falsche Einstellungen bei Berechtigungen interner oder externer Mitarbeiter (Berechtigungen in Bezug auf Person) (?) (go to 7.3.4. und 7.3.5.)
  (?) Benötigen Sie Hilfe? Die Datenschutzverletzung bezieht sich auf eine Situation, in der die Zugriffs- oder Leserechte eines Benutzers entweder nicht korrekt oder absichtlich falsch geändert wurden, wodurch der Benutzer mehr Rechte im System hat, als ihm zustehen. Z. B.: Bei einer Funktionsänderung wurde eine Berechtigungsrolle nicht korrekt umgesetzt, zu weit gefasste Zugriffsrechte, Administratorrechte für nicht autorisierte Personen usw.
- ☐ Netzwerkordner, -anwendungen oder -speicherorte mit personenbezogenen Daten sind innerhalb der Organisation zu weitreichend zugänglich eingerichtet (Dateiberechtigungen) (?) (go to 7.3.6; 7.3.7 und 7.3.8.)
  (?) Benötigen Sie Hilfe? Die Datenschutzverletzung bezieht sich auf eine Situation, in der ein (gemeinsam genutzter) Ordner, Speicherort oder eine Anwendung innerhalb der Organisation falsch konfiguriert und daher für interne unbefugte Personen sichtbar ist. Z. B.: Ein Ordner mit Personaldaten, der der Personalabteilung vorbehalten ist, war für jeden Mitarbeiter zugänglich.
- ☐ Netzwerkordner, -anwendungen oder -speicherorte mit personenbezogenen Daten, die von außerhalb der Organisation zugänglich sind (?) (go to 7.3.6; 7.3.7 und 7.3.8.)
  (?) Benötigen Sie Hilfe? Die Datenschutzverletzung bezieht sich auf eine Situation, in der eine Datei, ein Speicherort oder eine Anwendung mit dem Internet verbunden ist und für Unbefugte über das Internet zugänglich ist. Z. B.: Das Extranet einer Organisation ist für Unbefugte außerhalb der Organisation zugänglich.
- ☐ Gerät (Mobiltelefon, Tablet usw.), Datenträger (z. B. USB-Stick) und/oder Papier mit personenbezogenen Daten verloren (go to 7.3.9; 7.3.10 und 7.3.11)
- ☐ Gerät (Mobiltelefon, Tablet usw.), Datenträger (z. B. USB-Stick) und/oder Papier mit personenbezogenen Daten gestohlen (go to 7.3.9; 7.3.10 und 7.3.11)
- ☐ Personenbezogene Daten wurden unrechtmäßig veröffentlicht. (Z. B. Indizierung in einer Suchmaschine, Daten wurden auf einer Website, einer Social Media-Plattform oder einem Papierträger [Zeitung, Zeitschrift usw.] veröffentlicht.(?) (go to 7.3.12; 7.3.13. und 7.3.14.)
  (?) Benötigen Sie Hilfe? Die Datenschutzverletzung bezieht sich auf eine Situation, in der (eine Datei mit) personenbezogene(n) Daten versehentlich veröffentlicht wurde(n). Z. B.: Indexierung von Dateien in Suchmaschinen, Veröffentlichung nicht pseudonymisierter Entscheidungen, unbeabsichtigte Veröffentlichung personenbezogener Daten auf Social Media-Plattformen usw.
- ☐ Anzeige personenbezogener Daten der falschen Person im persönlichen Portal oder einer ähnlichen Umgebung (go to 7.3.15; 7.3.16 und 7.3.17.)
- ☐ Nicht (ordnungsgemäße) Vernichtung personenbezogener Daten (z. B. Entsorgung lesbarer personenbezogener Daten im Altpapier) (go to 7.3.18.)
- ☐ Unrechtmäßige Vernichtung personenbezogener Daten (go to 7.3.18.)
- ☐ DNS-Spoofing/Poisoning (?) (go to 7.3.19; 7.3.20; 7.3.21; 7.3.22)
  (?) Benötigen Sie Hilfe? DNS-Spoofing, auch als Cache Poisoning bezeichnet, ist eine Datenschutzverletzung, bei der ein Browser so manipuliert wird, dass Besucher einer

Website auf schädliche Websites umgeleitet werden, die darauf abzielen, sensible Informationen zu erlangen. DNS-Spoofing findet statt, wenn Ihr Cache mit diesen schädlichen Umleitungen infiziert wird.

- ☐ Phishing (go to 7.3.23; 7.3.24; 7.3.25; 7.3.26; 7.3.27; 7.3.28; 7.3.29)
- ☐ Ransomware (go to 7.3.30; 7.3.31;7.3.32;7.3.33 und 7.3.34)
- ☐ Credential Stuffing (?) (go to 7.3.35; 7.3.36 und 7.3.37)
  (?) Benötigen Sie Hilfe? Credential Stuffing ist die automatische Eingabe gestohlener Benutzernamen und Passwörter („Anmeldedaten“) in Anmeldeformularen von Websites, um sich auf betrügerische Weise Zugang zu Benutzerkonten zu verschaffen.
- ☐ SQL-Injection (?) (go to 7.3.38; 7.3.39; 7.3.40 und 7.3.41.)
  (?) Benötigen Sie Hilfe? SQL-Injektion (SQLi) ist eine Schwachstelle in der Websicherheit, durch die ein Angreifer die Abfragen einer Anwendung an deren Datenbank manipulieren kann. Dadurch kann ein Angreifer Daten einsehen, auf die er normalerweise keinen Zugriff hat. Dabei kann es sich um Daten handeln, die anderen Benutzern gehören, oder um andere Daten, auf die die Anwendung Zugriff hat. In vielen Fällen kann ein Angreifer diese Daten ändern oder löschen, wodurch der Inhalt oder das Verhalten der Anwendung dauerhaft verändert wird.
- ☐ (D)DOS-Angriff (?) (go to 07.03.2042; 07.03.2043 und 07.03.2044)
  (?) Benötigen Sie Hilfe? Ein Distributed-Denial-of-Service-Angriff (DDoS) ist ein böswilliger Versuch, den regulären Datenverkehr eines Servers, Dienstes oder Netzwerks zu beeinträchtigen, indem das Ziel oder die umgebende Infrastruktur mit einer Flut von Datenverkehr über das Internet überlastet wird.
- ☐ KI-Modelle (Leckage/Regurgitation usw.) (?)
  (?) Benötigen Sie Hilfe? Regurgitation ist das Phänomen, bei dem ein KI-Modell Antworten generiert, die den Trainingsdaten sehr ähnlich sind, wodurch möglicherweise sensible Informationen preisgegeben werden.
- ☐ Richtlinie zur koordinierten Offenlegung von Schwachstellen/Bug-Bounty (?)
  (?) Benötigen Sie Hilfe? Eine Richtlinie zur koordinierten Offenlegung von Schwachstellen (englisch:„Coordinated Vulnerability Disclosure Policy“ – CVDP) ist ein Satz von Regeln, die von einer für Informationssysteme verantwortlichen Organisation im Voraus festgelegt wurden, damit Teilnehmer (oder „ethische Hacker“) mit guter Absicht mögliche Schwachstellen in ihren Systemen aufspüren oder der Organisation alle relevanten Informationen dazu übermitteln können Ein Belohnungsprogramm zur Aufdeckung von Schwachstellen (englisch: „Bug Bounty“) umfasst alle Regelungen, die eine verantwortliche Organisation festgelegt hat, um Teilnehmern, die Schwachstellen in den von ihr eingesetzten Technologien entdecken, Belohnungen zu gewähren. Es handelt sich um eine Richtlinie zur koordinierten Offenlegung von Schwachstellen, die vorsieht, dass den Teilnehmern entsprechend der Menge, Bedeutung oder Qualität der bereitgestellten Informationen eine Belohnung gewährt wird.
- ☐ Sonstige: *Feld für freien Text*

E-Mail mit personenbezogenen Daten an falsche Empfänger gesendet

7.3.1. Hat der falsche Empfänger bestätigt, die E-Mail gelöscht zu haben und die personenbezogenen Daten nicht (weiter) zu verwenden?*

Dropdown:
Ja
Nein

E-Mail mit personenbezogenen Daten an Empfänger im Feld „An“ oder „Cc“ statt „Bcc“ gesendet

7.3.2. Haben Sie eine (neue) E-Mail an die Empfänger in Bcc gesendet, in der Sie darum gebeten haben, die vorherige E-Mail zu löschen und die personenbezogenen Daten nicht (weiter) zu verwenden?*

Dropdown:
Ja
Nein

Brief oder Paket mit personenbezogenen Daten an den falschen Empfänger gesendet oder zugestellt

7.3.3. Hat der falsche Empfänger bestätigt, dass die personenbezogenen Daten vernichtet oder zurückgesendet wurden?

Dropdown:
Ja
Nein

Falsche Einstellungen bei Berechtigungen interner oder externer Mitarbeiter (Berechtigungen in Bezug auf Person)

7.3.4. Haben Sie den internen oder externen Mitarbeiter darauf hingewiesen, dass die Informationen nicht für andere Zwecke weiterverwendet werden dürfen?*

Dropdown:
Ja
Nein

7.3.5. Wurden von dem internen oder externen Mitarbeiter Kopien von Dokumenten angefertigt, die personenbezogene Daten enthielten, zu denen dieser Mitarbeiter nicht berechtigt war?*

Dropdown:
Ja (go to 7.3.5.1.)
Nein
Nicht bekannt

7.3.5.1. Wurden die Kopien wiederhergestellt?

Dropdown:
Ja
Nein

Netzwerkordner, -anwendungen oder -speicherorte mit personenbezogenen Daten sind innerhalb der Organisation zu weitreichend zugänglich eingerichtet (Dateiberechtigungen), und Netzwerkordner, -anwendungen oder -speicherorte mit personenbezogenen Daten sind von außerhalb der Organisation zugänglich

7.3.6. Kann anhand von Protokoll-Dateien oder ähnlichen Einstellungen überprüft werden, wie viele Personen Zugriff auf die Netzwerkordner, -anwendungen oder -speicherorte erhalten haben?*

Dropdown:
Ja (go to 7.3.6.1.)
Nein

7.3.6.1. Wie viele Personen hatten unrechtmäßigen Zugriff auf die Netzwerkordner, -anwendungen oder -speicherorte?*

Zahlenfeld

7.3.7. Kann anhand von Protokollen oder ähnlichen Einstellungen überprüft werden, wann Personen Zugriff auf die Netzwerkordner, -anwendungen oder -speicherorte erhalten haben?*

Dropdown:
Ja (go to 7.3.7.1.)
Nein

7.3.7.1. Wann fand der erste unberechtigte Zugriff statt?*

Datumsfeld	*Stundenfeld*

7.3.8. Kann überprüft werden, ob Downloads oder ähnliche Kopien der in den Netzwerkordnern, -anwendungen oder -speicherorten enthaltenen Informationen vorgenommen wurden?*

Dropdown:
Ja (go to 7.3.8.1.)
Nein

7.3.8.1. Wurden die Downloads oder ähnliche Kopien wiederhergestellt?*

Dropdown:
Ja
Nein

Gerät (Mobiltelefon, Tablet usw.), Datenträger (z. B. USB-Stick) und/oder Papier mit personenbezogenen Daten verloren und Gerät (Mobiltelefon, Tablet usw.), Datenträger (z. B. USB-Stick) und/oder Papier mit personenbezogenen Daten gestohlen

7.3.9. War das Gerät oder der Datenträger mit MFA gesichert?*

Dropdown:
Ja
Nein (go to 7.3.9.1.)

7.3.9.1. War das Gerät oder der Datenträger mit einem Passwort geschützt?

Dropdown:
Ja
Nein

7.3.10. Waren die personenbezogenen Daten auf dem Gerät oder Datenträger durch Verschlüsselung, Hash-Funktionen oder ähnliche Techniken unlesbar gemacht?

Dropdown:
Ja (go to 7.3.10.1)
Nein

7.3.10.1. Welches konkrete Verschlüsselungsprotokoll, welche Hash-Funktion oder welche ähnliche Technik wurde verwendet?*

Mehrere Antworten möglich

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Sonstige: *Feld für freien Text**

7.3.11. Wurden die Daten auf dem Gerät inzwischen aus der Ferne gelöscht?*

Dropdown:
Ja
Nein

Personenbezogene Daten wurden unrechtmäßig veröffentlicht. /Z. B. Indizierung in einer Suchmaschine, Daten wurden auf einer Website, einer Social Media-Plattform oder einem

Papierträger [Zeitung, Zeitschrift usw.] veröffentlicht.

7.3.12. Wo (Ort) wurden die personenbezogenen Daten genau veröffentlicht?*

Feld für freien Text

7.3.13. Sind die unrechtmäßig veröffentlichten personenbezogenen Daten noch zugänglich?*

Dropdown:
Ja
Nein (go to 7.3.13.1.)

7.3.13.1. Wie lange waren die zu Unrecht veröffentlichten personenbezogenen Daten zugänglich?*

Von*		Bis*	
Datum	*Uhrzeit*	*Datum*	*Uhrzeit*

7.3.14. Kann überprüft werden, wie viele Personen unrechtmäßig Kenntnis von den zu Unrecht veröffentlichten personenbezogenen Daten genommen haben?*

Dropdown:
Ja (go to 7.3.14.1.)
Nein

7.3.14.1. Wie viele Personen haben Kenntnis von den unrechtmäßig veröffentlichten personenbezogenen Daten genommen?*

Anzahl der Personen: Zahl

Personenbezogene Daten der falschen Person im persönlichen Portal oder in einer ähnlichen Umgebung angezeigt

7.3.15. Was war die Ursache (Systemaktualisierung, Fehler, falsche Einstellung, Homonymie usw.), die dazu führte, dass die Person oder Personen personenbezogene Daten eines anderen Betroffenen sehen konnten?*

Feld für freien Text

7.3.16. Haben Sie die Personen darauf hingewiesen, dass sie die personenbezogenen Daten der anderen Betroffenen nicht weiter verwenden dürfen?*

Dropdown:
Ja
Nein

7.3.17. Wurden die betroffenen Personen, deren personenbezogene Daten den anderen Personen unrechtmäßig angezeigt wurden, darüber informiert?*

Dropdown:
Ja
Nein

Keine oder nicht ordnungsgemäße Vernichtung personenbezogener Daten (z. B. Entsorgung lesbarer Daten im Altpapier) und unrechtmäßige Vernichtung personenbezogener Daten

7.3.18. Verfügen Sie über eine Richtlinie/ein Verfahren zur Vernichtung personenbezogener Daten?*

Dropdown:
Ja
Nein

DNS-Spoofing/Poisoning

7.3.19. Verfügen Sie über die Webadresse und/oder IP-Adresse des Klons?*

Dropdown:
Ja (go to 7.3.19.1)
Nein

7.3.19.1. Bitte geben Sie die Web- oder IP-Adresse des Klons ein

Feld für freien Text

7.3.20. Verwendet Ihre Website das Transport Layer Security Protocol (TLS)?*(?)

(?) Benötigen Sie Hilfe? TLS-Protokoll verwenden: Das TLS-Protokoll (Transport Layer Security) ist ein kryptografisches Protokoll, das eine sichere Kommunikation über ein Netzwerk wie das Internet ermöglicht. Es verschlüsselt Daten und sorgt für Authentifizierung und Integrität, sodass Informationen wie Passwörter, Kreditkartendaten und E-Mails vor Abhören und Manipulation geschützt sind.

Dropdown:
Ja
Nein

7.3.21. Verfügt Ihre Website über ein funktionierendes SSL-Zertifikat?*(?)

(?) Benötigen Sie Hilfe? SSL-Zertifikat: Ein SSL-Zertifikat (Secure Sockets Layer) ist ein digitales Zertifikat, das eine sichere Kommunikation zwischen einer Website und einem Benutzer ermöglicht. Es verschlüsselt Daten wie Passwörter und Kreditkarteninformationen und stellt sicher, dass die Verbindung zuverlässig ist. SSL-Zertifikate bestätigen auch die Identität der Website.

Dropdown:
Ja
Nein

7.3.22. Verwendet Ihre Website die Domain Name System Security Extension? (DNSSEC)*(?)

(?) Benötigen Sie Hilfe? DNSSEC: DNSSEC (Domain Name System Security Extensions) ist eine Erweiterung des DNS-Systems, die für zusätzliche Sicherheit sorgt, indem sie über DNS abgerufene Daten überprüft. Es verhindert Angriffe wie „Cache Poisoning“, indem es überprüft, ob die empfangenen DNS-Daten echt und nicht manipuliert sind.

Dropdown:
Ja
Nein

Phishing

7.3.23. Über welchen Kanal erfolgte das Phishing?* (?)

(?) Benötigen Sie Hilfe?

- *Vishing: Phishing(-Versuche) über Telefonanrufe.*
- *Smishing: Phishing (Versuche) über SMS-Nachrichten*

Dropdown:
E-Mail-Verkehr
Vishing:
Smishing und Phishing über andere Nachrichtenplattformen (WhatsApp, Telegram, Signal usw.)

7.3.24. Um welchen Art von Phishing handelt es sich?* (?)

(?) Benötigen Sie Hilfe?

Spearphishing: Spearphishing greift eine bestimmte Person oder Organisation an, oft mit Inhalten, die auf das Opfer oder die Opfer zugeschnitten sind. Vor einem Spearphishing-Angriff ist in der Regel Aufklärungsarbeit erforderlich, um Namen, Funktionsbezeichnungen, E-Mail-Adressen und Ähnliches zu ermitteln. Die Hacker durchsuchen das Internet, um diese Informationen mit anderen recherchierten Informationen über die Kollegen des Opfers sowie den Namen und Arbeitsbeziehungen wichtiger Mitarbeiter in dessen Organisation zu verknüpfen. Auf diese Weise erstellt der Phishing-Angreifer eine glaubwürdige Phishing-Nachricht.

Whaling/CEO-Fraud: Phishing, das sich an einen hochrangigen Entscheidungsträger in der Organisation richtet. CEO-Fraud (oder Whaling) ist eine Form der Cyberkriminalität, bei der ein Betrüger eine E-Mail von einem hochrangigen Mitarbeiter wie einem CEO oder CFO versendet. Das Ziel ist es, Menschen dazu zu bringen, Geld auf das Bankkonto des Betrügers zu überweisen. CEO-Fraud ist also auch eine Form von Zahlungsbetrug.

Clone-Phishing: Ein Phishing-Angriff, bei dem der Angreifer eine Kopie einer legitimen Website oder E-Mail erstellt, um Benutzer dazu zu verleiten, ihre persönlichen Daten einzugeben. Bei diesem Angriff erstellen Kriminelle eine Kopie oder einen Klon zuvor versendeter legitimer E-Mails, die einen Link oder einen Anhang enthalten. Anschließend ersetzt der Phishing-Angreifer die Links oder Dateien im Anhang durch schädliche Ersatzdateien, die als die ursprünglichen Links oder Dateien getarnt sind.

Scareware: Z. B. eine E-Mail-Nachricht, in der Ihnen mitgeteilt wird, dass Sie ein Pädophiler sind und die Polizei weiß, dass Sie die Website X besucht haben; E-Mail-Nachricht, in der darauf hingewiesen wird, dass Sie Ihr Bankkonto bestätigen müssen, da Sie sonst keinen Zugriff mehr auf das Bankkonto X haben; E-Mail-Nachricht, in der „dringende Maßnahmen“ gefordert werden

Dropdown:
Spearphishing
Whaling/CEO-Fraud
Clonephishing
Scareware
Spoofing
Andere Arten von Phishing

7.3.25. Hat der von Phishing Betroffene Zugangsdaten (Benutzername, Passwort usw.) eingegeben?*

Dropdown:
Ja
Nein

7.3.26. Verfügte das kompromittierte Konto zum Zeitpunkt der Datenschutzverletzung über MFA?* (?)

(?) Benötigen Sie Hilfe? Multi-Faktor-Authentifizierung: MFA (Multi-Faktor-Authentifizierung) ist eine Sicherheitsmethode, bei der Sie mehrere Methoden zur Bestätigung Ihrer Identität verwenden, z. B. ein Passwort und einen Code, der an Ihr Smartphone gesendet wird.

Dropdown:
Ja
Nein

7.3.27. Verfügte das kompromittierte Konto zum Zeitpunkt der Datenschutzverletzung über ein Warnsystem oder ein ähnliches Benachrichtigungssystem, das eine Meldung generiert, wenn eine Anmeldung (oder ein Anmeldeversuch) von einem verdächtigen/unbekannten Standort aus erfolgt?*

Dropdown:
Ja
Nein

7.3.28. Wurden von dem kompromittierten Konto aus neue Phishing-E-Mails/Nachrichten versendet?*

Dropdown:
Ja (go to 7.3.28.1 und 7.3.28.2)
Nein
Nicht bekannt (go to 7.3.28.2)

7.3.28.1. Wie viele Phishing-E-Mails/Nachrichten wurden von dem kompromittierten Konto versendet?*

Dropdown:
Die genaue Anzahl der versendeten Phishing-E-Mails ist bekannt: *Anzahl*
Die genaue Anzahl der versendeten Phishing-E-Mails ist nicht bekannt, wird jedoch auf folgende Anzahl geschätzt: *Anzahl*

7.3.28.2. Haben Sie eine Warnnachricht an die Empfänger der Phishing-Mails/Nachrichten aus dem kompromittierten Konto gesendet, sofern Ihnen eine Empfängerliste vorliegt? Sofern Ihnen keine Empfängerliste vorliegt: Haben Sie eine Warnnachricht an alle Kontaktpersonen gesendet?*

Dropdown:
Ja
Nein

7.3.29. Haben Sie oder eine externe Partei eine Untersuchung zur Ursache und/oder zum Umfang der Datenschutzverletzung durchgeführt, z. B. zu welchen Dokumenten, E-Mails und anderen Orten mit dem kompromittierten Konto einschließlich der darin enthaltenen personenbezogenen Daten unbefugter Zugriff gewährt werden konnte?*

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.3.29.1.)

7.3.29.1. Datum, an dem die Ergebnisse der Untersuchung der Datenschutzverletzung voraussichtlich vorliegen werden*

Datumsfeld

Ransomware

7.3.30. Hat die Ransomware-Gruppe/der Hacker eine Ransomware-Mitteilung hinterlassen?*

Dropdown
Ja
Nein

7.3.31. Verfügt die Organisation über ein nicht kompromittiertes Backup nach dem Ransomware-Angriff?*

Dropdown:
Ja
Nein
Kann (zum jetzigen Zeitpunkt) nicht mit Sicherheit festgelegt werden

7.3.32. Wurde unrechtmäßig auf personenbezogene Daten zugegriffen?*

Dropdown:
Ja (go to 7.3.32.1.)
Nein
Kann (zum jetzigen Zeitpunkt) nicht mit Sicherheit festgestellt werden (go to 7.3.32.1.)

7.3.32.1. Wurden die personenbezogenen Daten, auf die (möglicherweise) zugegriffen wurde, vor dem Zugriff verschlüsselt, gehasht oder anderweitig unlesbar gemacht?*

Dropdown:
Ja (go to 7.3.32.1.1)
Nein

7.3.32.1.1. Welches konkrete Verschlüsselungsprotokoll, welche Hash-Funktion oder welche ähnliche Technik wurde verwendet?*

Mehrere Antworten möglich

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Sonstige: *Feld für freien Text**

7.3.33. Gab es eine Exfiltration personenbezogener Daten?*

Dropdown:
Ja (go to 7.3.33.1.)
Nein
Kann (zum jetzigen Zeitpunkt) nicht mit Sicherheit festgestellt werden (go to 7.3.33.1.)

7.3.33.1. Wurden die (möglicherweise) exfiltrierten personenbezogenen Daten vor der Exfiltration verschlüsselt, gehasht oder anderweitig unlesbar gemacht?*

Dropdown:
Ja (go to 7.3.33.1.1.)
Nein

7.3.33.1.1. Welches konkrete Verschlüsselungsprotokoll, welche Hash-Funktion oder welche ähnliche Technik wurde verwendet?*

Mehrere Antworten möglich

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Sonstige: *Feld für freien Text**

7.3.34. Haben Sie oder eine externe Partei eine Untersuchung zur Ursache und/oder zum Umfang der Datenschutzverletzung durchgeführt, z. B. auf welche Dokumente, E-Mails und andere Speicherorte (möglicherweise) unbefugt zugegriffen wurde und/oder welche personenbezogenen Daten (möglicherweise) exfiltriert wurden?

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.3.34.1.)

7.3.34.1. Datum, an dem die Ergebnisse der Untersuchung der Datenschutzverletzung voraussichtlich vorliegen werden*

Datumsfeld

Credential Stuffing

7.3.35. Verfügten die Konten, auf die infolge des Credential Stuffing-Angriffs zugegriffen wurde, über MFA?*(?)

(?) Benötigen Sie Hilfe? Multi-Faktor-Authentifizierung: MFA (Multi-Faktor-Authentifizierung) ist eine Sicherheitsmethode, bei der Sie mehrere Methoden zur Bestätigung Ihrer Identität verwenden, z. B. ein Passwort und einen Code, der an Ihr Smartphone gesendet wird.

Dropdown:
Ja
Nein (go to 7.3.35.1.; 7.3.35.2; 7.3.35.3 und 7.3.35.4)

7.3.35.1. Ist bei der Anmeldung zu Konten ein CAPTCHA oder ein ähnlicher Test vorgesehen?*

Dropdown
Ja
Nein

7.3.35.2. Wendet Ihre Organisation IP-Blocking an, wie z. B. Geo-Blocking oder das Blacklisting bestimmter IP-Adressen?*

Dropdown
Ja
Nein

7.3.35.3. Sieht Ihre Organisation eine maximale Anzahl von Anmeldeversuchen innerhalb eines bestimmten Zeitraums von einer bestimmten IP-Adresse aus für ein Konto oder eine ähnliche Beschränkung vor?*

Dropdown
Ja
Nein

7.3.35.4. Verfügt Ihre Organisation über andere Präventionsmaßnahmen, um Credential Stuffing zu verhindern?*

Feld für freien Text

7.3.36. Haben Sie die Betroffenen der kompromittierten Konten darüber informiert, dass ein (versuchter) unrechtmäßiger Zugriff auf ihre Konten stattgefunden hat und dass, wenn sie dieselben Zugangsdaten auch anderswo verwenden, diese möglicherweise ebenfalls kompromittiert sind?*

Dropdown
Ja
Nein

7.3.37. Haben Sie oder eine externe Partei eine Untersuchung zur Ursache und/oder zum Umfang der Datenschutzverletzung durchgeführt?*

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.3.37.1.)

7.3.37.1. Datum, an dem die Ergebnisse der Untersuchung der Datenschutzverletzung voraussichtlich vorliegen werden*

Datumsfeld

SQL-Injection

7.3.38. Verwenden Sie Prepared Statements/parametrisierte Abfragen?*

Dropdown
Ja
Nein

7.3.39. War es möglich, von außerhalb als Root-User eine Verbindung zur Anwendung herzustellen?*

Dropdown
Ja
Nein

7.3.40. Verwenden Sie Sanitization Libraries oder andere Mechanismen, um die Daten in der Datenbank zu bereinigen?*

Dropdown
Ja
Nein

7.3.41. Haben Sie oder eine externe Partei eine Untersuchung zur Ursache und/oder zum Umfang der Datenschutzverletzung durchgeführt?*

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.3.41.1.)

7.3.41.1. Datum, an dem die Ergebnisse der Untersuchung der Datenschutzverletzung voraussichtlich vorliegen werden*

Datumsfeld

(D)DOS-Angriff

7.3.42. War es während des DDOS-Angriffs für berechtigte Benutzer weiterhin möglich, eine Verbindung zum betroffenen Server herzustellen?*

Dropdown
Ja
Nein (go to 7.3.42.1.)

7.3.42.1. War der betroffene Server länger als 24 Stunden nicht verfügbar?*

Dropdown			
Ja			
Nein			
Ausfallzeit Anfang*		Ausfallzeit Ende*	
Datumsfeld	*Stundenfeld*	*Datumsfeld*	*Stundenfeld*

7.3.43. Verfügen Sie über SIEM- (Security Information and Event Management), EDR- (Endpoint Detection and Response) und/oder XDR-Anwendungen (Extended Detection and Response), um den Datenverkehr zu überwachen und darauf zu reagieren?*

Dropdown
Ja (go to 7.3.43.1.)
Nein

7.3.43.1. Bitte geben Sie an, über welche SIEM-, EDR- und/oder XDR-Anwendungen Ihre Organisation verfügt*

Feld für freien Text

7.3.44. Haben Sie oder eine externe Partei eine Untersuchung zur Ursache und/oder zum Umfang der Datenschutzverletzung durchgeführt?*

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.3.44.1.)

7.3.44.1. Datum, an dem die Ergebnisse der Untersuchung der Datenschutzverletzung voraussichtlich vorliegen werden*

Datumsfeld

7.4. Zusammenfassung der Datenschutzverletzung* (?)

(?) Benötigen Sie Hilfe? Zusammenfassung der Datenschutzverletzung: Geben Sie bei der Zusammenfassung der Datenschutzverletzung weitere Informationen zu folgenden Punkten an:

- *Ursache, Art, Typ und Umstände der Datenschutzverletzung*
- *Zeitpunkt und Feststellung der Datenschutzverletzung*
- *Beschreibung der (betroffenen) Verarbeitung und der betroffenen personenbezogenen Daten*
- *Bisher ergriffene Maßnahmen und getroffene Entscheidungen (Zeitleiste)*

Feld für freien Text – maximal 2500 Zeichen

7.5. Hat der DPO eine Empfehlung zur Meldung der Datenschutzverletzung, zur gegebenenfalls erforderlichen Mitteilung an die Betroffenen und/oder zu den zu ergreifenden Maßnahmen abgegeben?

Dropdown:
Ja
Nein
Untersuchung noch nicht abgeschlossen (go to 7.5.1.)

7.5.1. Bitte geben Sie die Empfehlung des DPOs an.*

Feld für freien Text – maximal 500 Zeichen

8. Management

8.1. Welche spezifischen (technischen und organisatorischen) Maßnahmen wurden getroffen, um die betroffenen personenbezogenen Daten zu schützen/diese Art von Datenschutzverletzung zu verhindern? (?)

(?) Benötigen Sie Hilfe? Welche spezifischen (technischen und organisatorischen) Maßnahmen wurden getroffen, um die betroffenen personenbezogenen Daten zu schützen/diese Art von Datenschutzverletzung zu verhindern?

Bitte beschreiben Sie nur die Maßnahmen, die unmittelbar zur Verhinderung der Datenschutzverletzung relevant sind, und geben Sie keinen allgemeinen Überblick über alle Maßnahmen.

Z. B.: Pseudonymisierung, Aggregation, Hashing, Audit-Protokolle, Multi-Faktor-Authentifizierung, Datenabschirmung/Trennung/Identitäts- und Berechtigungssystem, Remote Wipe, Verschlüsselung, Firewall, Passwörter usw.

Bestehende technische Maßnahme*	Bestehende organisatorische Maßnahme*
Hinzufügen	Hinzufügen
Maßnahme	*Maßnahme*
+	+

8.2. Welche spezifischen neuen/zusätzlichen (technischen und organisatorischen) Maßnahmen wurden als Reaktion auf die Datenschutzverletzung ergriffen? (?)

(?) Benötigen Sie Hilfe? Welche spezifischen neuen/zusätzlichen (technischen und organisatorischen) Maßnahmen wurden als Reaktion auf die Datenschutzverletzung ergriffen?

Bitte beschreiben Sie nur Maßnahmen, die als Reaktion auf die tatsächlich stattgefundene Datenschutzverletzung ergriffen wurden, und geben Sie keine Übersicht über alle Maßnahmen.

Z. B.: Erfassung des Umfangs der Datenschutzverletzung, Einstellung der gesamten oder teilweisen Verarbeitung personenbezogener Daten, Änderungen der Zugriffsrechte, Änderung der Standard-Administratoren und/oder Benutzerpasswörtern, Änderung von Administratoren und/oder Authentifizierungsmitteln der Benutzer, Inanspruchnahme technischer Unterstützung (bitte Stelle angeben), Meldung der Datenschutzverletzung an den Verantwortlichen einer verbundenen Anwendung, Unterbrechung oder Absicherung der Verknüpfung mit anderen Anwendungen, erneute Indexierung oder De-Indexierung der kompromittierten Daten, Löschen (Wipen) mit Bestätigung durch das Gerät und Bestätigungssignal über die erfolgreiche Aktion, Änderung des Verschlüsselungssystems, Meldung an die zuständigen Aufsichts- bzw. Strafverfolgungsbehörden (bitte angeben), erfolgreiche Aktualisierung (Patchen) der Systeme usw. Geben Sie auch das Datum der Umsetzung an.

Technische Maßnahmen*		Organisatorische Maßnahmen*	
Hinzufügen		Hinzufügen	
Maßnahme	*Datum*	*Maßnahme*	*Datum*
+	+	+	+

8.3. Welche spezifischen neuen/zusätzlichen (technischen und/oder organisatorischen) Maßnahmen werden in Zukunft (als Reaktion auf die Datenschutzverletzung) ergriffen? (?)

(?) Benötigen Sie Hilfe? Welche spezifischen neuen/zusätzlichen (technischen und/oder organisatorischen) Maßnahmen werden in Zukunft (als Reaktion auf die Datenschutzverletzung) ergriffen?

Bitte beschreiben Sie die künftigen Maßnahmen, die als Reaktion auf die konkret aufgetretenen Datenschutzverletzung ergriffen werden.

Z. B.: Einführung von MFA für alle Benutzer, Änderung der Active Directory-Struktur, Segmentierung des IT-Systems, Installation einer neuen Backup-Anwendung, Installation einer (neuen) EDR/XDR-Anwendung usw.. Geben Sie auch das voraussichtliche Datum der Umsetzung an.

Technische Maßnahmen*		Organisatorische Maßnahmen*	
Hinzufügen		Hinzufügen	
Maßnahme	*Datum*	*Maßnahme*	*Datum*
+	+	+	+

9. Risiko

9.1. Verfügt die Organisation über eine (allgemeine) Methode zur Auflistung und Bewertung (auf der Grundlage von Schwere und Wahrscheinlichkeit) der Risiken für die Rechte und Freiheiten natürlicher Personen im Falle einer Datenschutzverletzung im Zusammenhang mit personenbezogenen Daten?*

Dropdown
Ja (go to 9.1.1.)
Nein

9.1.1. Welche Methode verwenden Sie hierfür (ENISA, selbst entwickelte Methode, andere usw.)**

Dropdown
ENISA
Selbst entwickelte Methode
Andere wie CRAMM, OWASP, FAIR Privacy, NIST Privacy Risk Assessment Matrix (PRAM)

9.2. Ergebnis der Analyse hinsichtlich des Risikos/der Risiken für die Rechte und Freiheiten der Betroffenen*

Dropdown
Wahrscheinlich hohes Risiko
Wahrscheinliches Risiko
Wahrscheinlich kein Risiko

9.3. Auswirkungen/Folgen für die Betroffenen*

- ☐ Verlust der Kontrolle über personenbezogene Daten
- ☐ Verlust der Vertraulichkeit personenbezogener Daten, die durch das Berufsgeheimnis (gemäß Art. 458 Strafgesetzbuch) geschützt sind
- ☐ Verletzung der physischen Unversehrtheit
- ☐ Verletzung der psychischen Unversehrtheit
- ☐ Verletzung der Privatsphäre (sexuelle Orientierung, Nacktfotos usw.)
- ☐ Ausnutzung einer schwachen Position (z. B. Minderjährige, ältere Menschen, Menschen mit Behinderung usw.)
- ☐ Materieller Schaden
- ☐ Immaterieller Schaden
- ☐ Vorübergehende Verhinderung des Zugangs zu Dienstleistungen
- ☐ Dauerhafte Verhinderung des Zugangs zu Dienstleistungen
- ☐ Diskriminierung
- ☐ Identitätsdiebstahl oder -betrug
- ☐ Finanzielle Verluste
- ☐ Unbefugte Aufhebung der Pseudonymisierung
- ☐ Reputationsschaden
- ☐ Einschränkung der Bewegungsfreiheit (z. B. Verweigerung der Grenzüberquerung)
- ☐ Sonstige erhebliche wirtschaftliche oder soziale Nachteile (go to 9.3.1.)
- ☐ Einschränkung anderer Freiheiten (go to 9.3.2.)
- ☐ Einschränkung anderer Rechte (go to 9.3.3.)
- ☐ Sonstige Auswirkungen (go to 9.3.4.)

9.3.1. Bitte erläutern Sie sonstige erhebliche wirtschaftliche oder soziale Nachteile*

Feld für freien Text

9.3.2. Bitte erläutern Sie die Einschränkung anderer Freiheiten*

Feld für freien Text

9.3.3. Bitte erläutern Sie die Einschränkung anderer Rechte*

Feld für freien Text

9.3.4. Bitte erläutern Sie andere Auswirkungen*

Feld für freien Text

10. Mitteilung (?)

(?) Benötigen Sie Hilfe? Bereitstellung von Informationen: Meldung an die Betroffenen bei Datenschutzverletzungen:

Die GBA empfiehlt eine Meldung an die Betroffenen bei Datenschutzverletzungen, die sich auf Folgendes beziehen:

- *Besondere Kategorien personenbezogener Daten (Art. 9.1 DSGVO).*
- *Strafrechtliche Daten (Art. 10 DSGVO).*
- *Kopien von Ausweisdokumenten/Pässen oder nationale Identifikationsnummern.*
- *Daten von besonders schutzbedürftigen Gruppen (z. B. Minderjährige).*
- *Große Datenmengen oder eine große Anzahl Betroffener.*

Dies kann zu Folgendem führen:

- *Diskriminierung, Identitätsbetrug, finanzielle Verluste oder Rufschädigung.*
- *Verletzung der Privatsphäre, des Berufsgeheimnisses oder erhebliche Auswirkungen auf Rechte und Freiheiten.*

Empfehlungen der GBA (Art. 34 DSGVO):

- *Sind die individuellen Kontaktdaten der betroffenen Personen verfügbar, muss grundsätzlich eine individuelle Benachrichtigung erfolgen – unabhängig von der Anzahl der betroffenen Personen.*
- *Eine öffentliche Bekanntmachung, wie beispielsweise ein Banner auf der Website, sollte ebenso wirksam sein wie eine individuelle Mitteilung.*
- *Maßnahmen zur Verhinderung künftiger Verstöße reichen nicht aus; nur Maßnahmen, die die Risiken des aktuellen Verstoßes begrenzen, sind zulässig, um sich auf die Ausnahmeregelung in Art. 34 DSGVO zu berufen.*

Inhalt der Meldung: Die Meldung muss:

- *Spezifische Kategorien betroffener Daten benennen, um die Betroffenen über Risiken zu informieren.*
- *Vorschläge für Maßnahmen enthalten, die die Betroffenen selbst ergreifen können.*

Phishing-Vorfälle: Bei Phishing müssen möglicherweise drei Gruppen informiert werden:

- *Die Personen, die Phishing-E-Mails erhalten haben, und der Inhaber des gehackten E-Mail-Kontos.*
- *Personen, deren Daten in E-Mails oder Anhängen der gehackten Mailbox enthalten sind.*

10.1. Haben Sie die Datenschutzverletzung bereits den Betroffenen gemeldet?*

Dropdown:
Ja (go to 10.1.1.)
Nein (go to 10.2. und 10.3.)

10.1.1. Haben Sie die Betroffenen individuell informiert?*

Dropdown:
Ja (go to 10.1.1.1.; 10.1.1.2.; 10.1.1.3.)
Nein (go to 10.1.1.4.; 10.1.1.5. und 10.3.)

10.1.1.1. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen individuell zu informieren?*

- ☐ Telefonisch
- ☐ Per Brief
- ☐ Per E-Mail
- ☐ Anderer Kanal. *(Feld für freien Text)*

10.1.1.2. Wie vielen Betroffenen haben Sie die Datenschutzverletzung individuell gemeldet?*

Anzahl

10.1.1.3. Wann haben Sie die Datenschutzverletzung den Betroffenen individuell gemeldet?*

Datumsfeld: Kalender

10.1.1.4. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen kollektiv zu informieren? *

- ☐ Über eine Mitteilung auf der Website
- ☐ Über soziale Medien
- ☐ Über eine Anzeige in der Zeitung
- ☐ Sonstiger Kanal: *(Feld für freien Text)*

10.1.1.5. Wann haben Sie die Datenschutzverletzung den Betroffenen kollektiv gemeldet?*

Datumsfeld: Kalender

10.2. Werden Sie die Datenschutzverletzung den Betroffenen noch melden?*

Dropdown:
Ja (go to 10.2.1.; 10.2.2.)
Nein (go to 10,3.)
Noch nicht bekannt (go to 10.3.)

10.2.1. Wann werden Sie den Betroffenen die Datenschutzverletzung (voraussichtlich) melden?*

Datumsfeld: Kalender

10.2.2. Werden Sie die Betroffenen individuell informieren?*

Dropdown:
Ja (go to 10.2.2.1; 10.2.2.2.)

Nein (go to 10.2.2.3; 10.2.2.4. und 10.3.)

10.2.2.1. Welches Kommunikationsmittel oder welchen Kommunikationskanal werden Sie verwenden, um die Betroffenen individuell zu informieren?*

- ☐ Telefonisch
- ☐ Per Brief
- ☐ Per E-Mail
- ☐ Sonstiger Kanal: *(Feld für freien Text)*

10.2.2.2. Wie vielen Betroffenen werden Sie die Datenschutzverletzung melden?*

Zahl/Anzahl

10.2.2.3. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen kollektiv zu informieren?*

- ☐ Über eine Mitteilung auf der Website
- ☐ Über soziale Medien
- ☐ Über eine Anzeige in der Zeitung
- ☐ Sonstiger Kanal: *(Feld für freien Text)*

10.2.2.4. Wie vielen Betroffenen werden Sie die Datenschutzverletzung melden?*

Zahl/Anzahl

10.3. Bitte geben Sie den Grund an, warum Sie auf die (individuellen) Mitteilung an die Betroffenen, deren personenbezogene Daten von der Datenschutzverletzung beeinträchtigt sind, absehen*

Mehrere Antworten möglich

- ☐ Weil wir der Meinung sind, dass wahrscheinlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht
- ☐ Es wäre mit unverhältnismäßigem Aufwand verbunden, jeden Betroffenen individuell zu informieren (go to 10.3.1.)
- ☐ Vor der Datenschutzverletzung wurden angemessene technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten getroffen (go to 10.3.2.)
- ☐ Nach der Datenschutzverletzung wurden Maßnahmen getroffen, die es unwahrscheinlich machen, dass tatsächlich ein hohes Risiko eintreten würde (go to 10.3.3.)
- ☐ Aufgrund vorgegebener Leitlinien anderer zuständiger Behörden, wie z. B. Strafverfolgungsbehörden (go to 10.3.4. und 10.3.5.)

10.3.1. Verfügen Sie über die individuellen (digitalen) Kommunikationsdaten der Betroffenen?*

Dropdown

Ja *Text: Die GBA geht davon aus, dass Sie, wenn Ihnen die individuellen Kommunikationsdaten der Betroffenen vorliegen, diese auch für eine individuelle Mitteilung nutzen müssen. Folglich kann die Ausnahmeregelung im Hinblick auf unverhältnismäßigen Aufwand keine Anwendung finden.*

Nein

10.3.2. Welche Maßnahmen haben Sie im Voraus getroffen, sodass es nicht erforderlich ist, die Betroffenen zu informieren?*

Feld für freien Text

10.3.3. Welche Maßnahmen haben Sie als Reaktion auf die Datenschutzverletzung getroffen, sodass es nicht erforderlich ist, die Betroffenen zu informieren?*

Feld für freien Text

10.3.4. Welche Behörde hat Leitlinien vorgegeben, wonach es (derzeit) nicht erforderlich/angebracht ist, die Betroffenen zu informieren?*

Feld für freien Text

10.3.5. Bitte fassen Sie den Inhalt der Leitlinie zusammen*

Feld für freien Text

11. Zusätzlich

Geben Sie hier alle Informationen an, die zum besseren Verständnis der Meldung beitragen können. (*Maximal 2000 Zeichen)*

Erklärung

☐ Indem Sie dieses Kästchen anklicken, erklären Sie, dass Sie befugt sind, diese Meldung abzugeben, und dass die in der Meldung gemachten Angaben korrekt sind.

12. Anhänge

Datiertes Exemplar der Mitteilung an die Betroffenen

Je nach Ihren Antworten handelt es sich um eine individuelle oder kollektive Mitteilung (siehe Registerkarte 10). Je nach Art und Umfang der Datenschutzverletzung müssen möglicherweise auch folgende Elemente in die Mitteilung an die Betroffenen aufgenommen werden:

- Bei personenbezogenen Daten der falschen Person, die im persönlichen Portal oder einer ähnlichen Umgebung angezeigt wurden: Die Tatsache, dass die personenbezogenen Daten der betroffenen Person anderen natürlichen Personen angezeigt wurden (siehe Registerkarte 7)
- Bei *Credential Stuffing*: Die Tatsache, dass ein (versuchter) unbefugter Zugriff auf das Konto der Betroffenen stattgefunden hat, und die Warnung dieser Betroffenen, dass diese Konten möglicherweise ebenfalls kompromittiert sein könnten (siehe Registerkarte 7), wenn sie dieselben *Credentials* auch anderswo verwenden

- Bei *Phishing*: Es muss eine Unterteilung in drei Gruppen von Betroffenen vorgenommen werden, die möglicherweise eine Mitteilung erhalten sollten:
    - Betroffene des E-Mail-Postfachs oder einer ähnlichen Umgebung selbst (siehe Registerkarte 7);
    - Betroffene, denen möglicherweise neue *Phishing*-Nachrichten zugesandt wurden (siehe Registerkarte 7)
    - Betroffene, deren personenbezogene Daten sich im E-Mail-Postfach oder einer ähnlichen Umgebung befanden (siehe Registerkarte 7).

Datiertes Exemplar der durchgeführten Risikobewertung

Wenn Sie eine Risikobewertung der betreffenden Datenschutzverletzung durchgeführt haben (siehe Registerkarte 9).

Datiertes Exemplar des Untersuchungsberichts

Wenn Sie oder ein Dritter die Ursache und/oder den Umfang der Datenschutzverletzung untersucht haben. Dies kann alle Arten von Datenschutzverletzungen betreffen (siehe Registerkarte 8). Die Datenschutzbehörde hält es für erforderlich, dass bei folgenden Arten von Datenschutzverletzungen eine Untersuchung durchgeführt und der entsprechende Bericht vorgelegt wird: DNS-Spoofing/Poisoning, Phishing, Ransomware, Credential Stuffing, SQL-Injection, (D)DoS-Angriff, KI-Modelle, Coordinated Vulnerability Disclosure Policy (siehe Registerkarte 7).

Datiertes Exemplar der Ransomware-Mitteilung

Wenn es sich um eine Art einer Ransomware-Datenschutzverletzung handelt und eine Ransomware-Mitteilung hinterlassen wurde (siehe Registerkarte 7).

Datiertes Exemplar der Phishing-Nachricht

Wenn es sich um eine Art einer *Phishing*-Datenschutzverletzung handelt und Ihnen noch die ursprüngliche Nachricht (Screenshot) vorliegt, mit der das *Phishing* durchgeführt wurde (siehe Registerkarte 7).

Datiertes Exemplar der Benachrichtigung über den verdächtigen Anmeldeversuch

Wenn es sich um eine Art *Phishing*-Datenschutzverletzung handelt und Ihnen die Benachrichtigung noch vorliegt, die vom Warnsystem für verdächtige Anmeldeversuche generiert wurde (siehe Registerkarte 7).

Datiertes Exemplar der Richtlinie zur Vernichtung personenbezogener Daten

Sofern Ihnen eine Richtlinie zur Vernichtung personenbezogener Daten vorliegt und es sich um folgende Arten von Datenschutzverletzungen handelt:

- Nicht (ordnungsgemäße) Vernichtung personenbezogener Daten (siehe Registerkarte 7)
- Unrechtmäßige Vernichtung personenbezogener Daten (siehe Registerkarte 7)

Datiertes Exemplar der Korrespondenz mit den falschen Empfängern

Abhängig von der Art der Datenschutzverletzung kann es sich um folgende Korrespondenz handeln:

- E-Mail, Brief oder Paket mit personenbezogenen Daten, das an den falschen Empfänger versandt wurde: Mitteilung mit der Aufforderung, die E-Mail, den Brief oder das Paket zu löschen bzw. zurückzusenden und die personenbezogenen Daten nicht (weiter) zu verwenden (siehe Registerkarte 7)

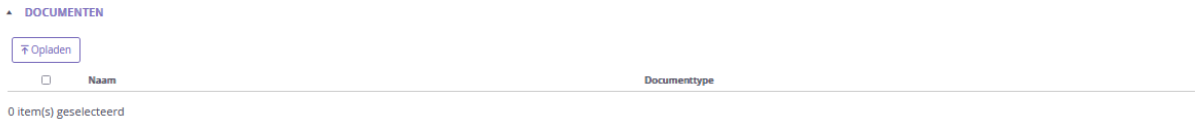
- E-Mail mit personenbezogenen Daten, die an Empfänger im Feld „An“ oder „Cc“ statt „Bcc“ gesendet wurde: Mitteilung mit der Aufforderung, die E-Mail zu löschen und die personenbezogenen Daten nicht (weiter) zu verwenden (siehe Registerkarte 7)
- Falsche Einstellungen von Berechtigungen für interne oder externe Mitarbeiter: Mitteilung an interne oder externe Mitarbeiter mit der Aufforderung, eventuelle Kopien zu löschen und die personenbezogenen Daten nicht (weiter) zu verwenden (siehe Registerkarte 7);
- Netzwerkordner, -anwendungen oder -speicherorte innerhalb oder außerhalb der Organisation zu weit gefasst: Mitteilung an interne oder externe Mitarbeiter oder Personen außerhalb der Organisation mit der Aufforderung, etwaige Kopien zu löschen und die personenbezogenen Daten nicht (weiter) zu verwenden (siehe Registerkarte 7);
- Personenbezogene Daten der falschen Person, die im persönlichen Portal oder einer ähnlichen Umgebung angezeigt werden: Mitteilung an die Person, die fälschlicherweise personenbezogene Daten des Betroffenen einsehen konnte, mit der Aufforderung, alle Kopien zu löschen und die personenbezogenen Daten nicht (weiter) zu verwenden (siehe Registerkarte 7).

Datiertes Exemplar der externen Meldung der Datenschutzverletzung

Wenn die Art der Feststellung der Datenschutzverletzung auf der Grundlage einer externen Meldung erfolgte (siehe Registerkarte 5).

Geben Sie an, welchen Anhang Sie bei der Einreichung der Meldung hochladen

☐ Datiertes Exemplar der Mitteilung an die Betroffenen
☐ Datiertes Exemplar der durchgeführten Risikobewertung
☐ Datiertes Exemplar des Untersuchungsberichts
☐ Datiertes Exemplar der Ransomware-Mitteilung
☐ Datiertes Exemplar der Phishing-Nachricht
☐ Datiertes Exemplar der Benachrichtigung über den verdächtigen Anmeldeversuch
☐ Datiertes Exemplar der Richtlinie zur Vernichtung personenbezogener Daten
☐ Datiertes Exemplar der Korrespondenz mit den falschen Empfängern
☐ Datiertes Exemplar der externen Meldung der Datenschutzverletzung



13. Abschließend

○ Ja, ich erkläre hiermit, dass Teil 2 vollständig ist
○ Nein, ich möchte meine Änderungen vorläufig speichern und das Formular später mit zusätzlichen Daten ergänzen (go to 13.1, wenn Sie auf „Änderungen speichern“ klicken)

13.1. Opgelet - Attention - Achtung

Indien u geen aanvullingen meer doet op deze tijdelijke bewaaropdracht, zullen de waardes die u hebt ingegeven binnen 21 dagen na het indienen van deel 1 als definitief worden beschouwd.

Si vous ne faites pas d'autres ajouts à cette notification temporaire, les valeurs que vous avez insérées seront considérées comme définitives dans un délai de 21 jours à compter de l'envoi de la partie 1.

Wenn Sie keine weiteren Ergänzungen zu dieser vorläufigen Mitteilung vornehmen, werden die von Ihnen eingegebenen Werte innerhalb von 21 Tagen nach Einreichung von Teil 1 als endgültig betrachtet.