Datenschutzbehörde

Felder zur Meldung von Datenschutzverletzungen TEIL 1

Inhalt

1. Informationen 4

Verifizierung: nur bei Einreichung ohne Konto (nur für belgische Unternehmen, die sich über ihre KBO-Nummer anmelden können – FAS) 6

2. Einführung 6

3. Organisation 6

3.1. Kontaktdaten des Verantwortlichen 6

3.2. Name der Organisation* 6

3.3. Hauptsitz 6

3.3.1. Unternehmensnummer 7

3.3.2. Land des Hauptsitzes* 7

3.3.3. Europäische Umsatzsteuer-Identifikationsnummer* 7

3.3.4. Eindeutiger Ländercode* 7

3.4. In welcher Branche ist der Verantwortliche tätig?* 7

3.4.1. Sonstige Branchen* 8

3.5. Adressdaten und Kontaktdaten des Verantwortlichen* (?) 8

3.6. E-Mail-Adresse des Verantwortlichen* (?) 8

3.7. Ist der Verantwortliche ein (Telekommunikations-)Betreiber, der beim BIPT registriert ist?* (?) 8

3.8. Ist der Verantwortliche ein börsennotiertes Unternehmen?* 8

3.9. Hat die Datenschutzverletzung bei einer Verarbeitung stattgefunden, die an einen Auftragsverarbeiter ausgelagert wurde?* 9

3.9.1. Um welchen Auftragsverarbeiter handelt es sich?* 9

3.10. Kontaktperson für die Datenschutzverletzung 9

4. International 9

4.1. Grenzüberschreitende Datenschutzverletzung 9

4.1.1. Hat die Datenschutzverletzung Auswirkungen auf Betroffene in mehreren Ländern?* 9

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 (?)* 10

4.2. Zuständige Aufsichtsbehörden in anderen EU-Mitgliedstaaten 10

4.2.1. Hat Ihre Organisation die Datenschutzverletzung anderen Datenschutzbehörden gemeldet?* 10

4.2.1.1. Bitte geben Sie an, in welchen Ländern Sie die Datenschutzverletzung den Datenschutzbehörden gemeldet haben* 10

5. Zeitleiste 10

5.1. Datum und Uhrzeit, zu denen die Datenschutzverletzung stattgefunden hat* . 10

5.1.1. Datum und Uhrzeit, zu denen die Datenschutzverletzung stattgefunden hat* 10

5.2. Datum und Uhrzeit, zu denen die Datenschutzverletzung festgestellt wurde* 11

5.3. Rechtfertigung für die verspätete Meldung der Datenschutzverletzung an die Datenschutzbehörde* 11

5.4. Wann wurde die Datenschutzverletzung behoben?* 11

5.4.1. Der Grund dafür ist:* 11

5.4.2. Wann wurde die Datenschutzverletzung behoben?* 11

6. Verarbeitung 11

6.1. Zwecke, für die die personenbezogenen Daten verarbeitet werden* 11

6.2. Art der von der Datenschutzverletzung beeinträchtigten personenbezogenen Daten* 11

6.3. Anzahl der Betroffenen, deren personenbezogene Daten beeinträchtigt wurden* 13

6.3.1. Ist die genaue Anzahl der Betroffenen bekannt?* 13

6.3.1.1. Anzahl der Personen/Betroffenen* 13

6.3.1.2. Mindest-/Höchstanzahl der Personen/Betroffenen* 13

7. Ursache 13

7.1. Art der Datenschutzverletzung* (?) 13

7.2. Zusammenfassung der Datenschutzverletzung* (?) 15

8. Mitteilung (?) 15

8.1. Haben Sie die Datenschutzverletzung bereits den Betroffenen gemeldet?* 16

8.1.1. Haben Sie die Betroffenen individuell informiert?* 16

8.1.1.1. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen individuell zu informieren?* 16

8.1.1.2. Wie vielen Betroffenen haben Sie die Datenschutzverletzung individuell gemeldet?* 17

8.1.1.3. Wann haben Sie die Datenschutzverletzung den Betroffenen individuell gemeldet?* 17

8.1.1.4. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen kollektiv zu informieren? * 17

8.1.1.5. Wann haben Sie die Datenschutzverletzung den Betroffenen kollektiv gemeldet?* 17

8.2. Werden Sie die Datenschutzverletzung den Betroffenen noch melden?* 17

8.2.1. Wann werden Sie den Betroffenen die Datenschutzverletzung (voraussichtlich) melden?* 17

8.2.2. Werden Sie die Betroffenen individuell informieren?* 17

8.2.2.1. Welches Kommunikationsmittel oder welchen Kommunikationskanal werden Sie verwenden, um die Betroffenen individuell zu informieren?* 17

8.2.2.2. Wie vielen Betroffenen werden Sie die Datenschutzverletzung melden?* .. 17

8.2.2.3. Welches Kommunikationsmittel oder welchen Kommunikationskanal haben Sie verwendet, um die Betroffenen kollektiv zu informieren?* 18

8.2.2.4. Wie vielen Betroffenen werden Sie die Datenschutzverletzung melden?*..18
9. Zusätzlich 18

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 bösartige 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.

Verifizierung: nur bei Einreichung ohne Konto (nur für belgische Unternehmen, die sich über ihre KBO-Nummer anmelden können – FAS)

Unternehmensnummer*

Bereits auf der Grundlage der Eingaben im Anmeldefluss ausgefüllt

Land*

Bereits ausgefüllt: Belgien

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

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

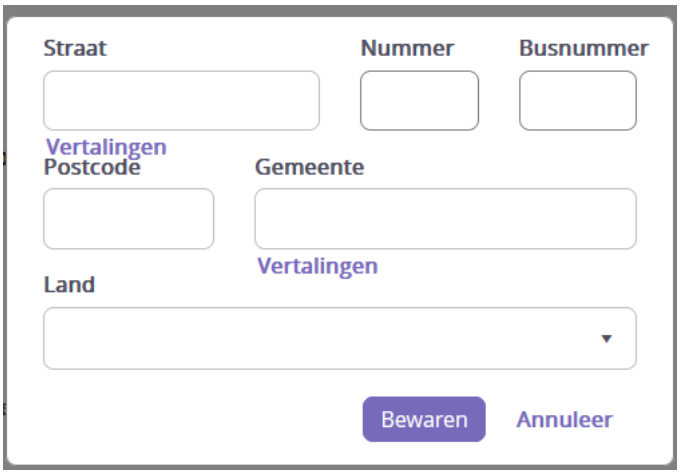
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen

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

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*

4.2. 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

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 5.3, falls zutreffend)	*Zeitfeld: Uhrzeit (go to 5.3, falls zutreffend)*

5.3. 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)

5.4. 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.)

5.4.1. Der Grund dafür ist:*

Feld für freien Text

5.4.2. 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

- ☐ 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

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

Besondere Kategorien personenbezogener Daten (Artikel 9.1 DSGVO)

- ☐ 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)

- ☐ 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.:

- ☐ 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*

7. Ursache

Was ist die Ursache für die Datenschutzverletzung?

7.1. 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.

- ☐ E-Mail mit personenbezogenen Daten an falsche Empfänger gesendet
- ☐ E-Mail mit personenbezogenen Daten an Empfänger im Feld „An“ oder „Cc“ statt „Bcc“ gesendet
- ☐ Brief oder Paket mit personenbezogenen Daten an den falschen Empfänger gesendet oder zugestellt
- ☐ Falsche Einstellungen bei Berechtigungen interner oder externer Mitarbeiter (Berechtigungen in Bezug auf Person) (?)
  (?) 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) (?)
  (?) 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 (?)
  (?) 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
- ☐ Gerät (Mobiltelefon, Tablet usw.), Datenträger (z. B. USB-Stick) und/oder Papier mit personenbezogenen Daten gestohlen
- ☐ 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.(?)
  (?) 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.
- ☐ Personenbezogene Daten der falschen Person im persönlichen Portal oder in einer ähnlichen Umgebung angezeigt
- ☐ Keine oder nicht ordnungsgemäße Vernichtung personenbezogener Daten (z. B. Entsorgung lesbarer personenbezogener Daten im Altpapier)
- ☐ Unrechtmäßige Vernichtung personenbezogener Daten
- ☐ DNS-Spoofing/Poisoning (?)
  (?) 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
- ☐ Ransomware
- ☐ Credential Stuffing (?)
  (?) 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 (?)
  (?) 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 (?)
  (?) 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*

7.2. 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

8. Mitteilung (?)

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

Die Datenschutzbehörde (DSB) empfiehlt, Betroffene bei Datenpannen zu informieren, die folgende Daten betreffen:

- *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.*

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

Dropdown:
Ja (go to 8.1.1.)
Nein (go to 8.2.)

8.1.1. Haben Sie die Betroffenen individuell informiert?*

Dropdown:
Ja (go to 8.1.1.1; 8.1.1.2; 8.1.1.3.)
Nein (go to 8.1.1.4; 8.1.1.5.)

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

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

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

Anzahl

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

Datumsfeld: Kalender

8.1.1.4. 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)*

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

Datumsfeld: Kalender

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

Dropdown:
Ja (go to 8.2.1; 8.2.2.)
Nein
Noch nicht bekannt

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

Datumsfeld: Kalender

8.2.2. Werden Sie die Betroffenen individuell informieren?*

Dropdown:
Ja (go to 8.2.2.1; 8.2.2.2.)
Nein (go to 8.2.2.3; 8.2.2.4.)

8.2.2.1. 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)*

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

Zahl/Anzahl

8.2.2.3. 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)*

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

Zahl/Anzahl

9. 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.

Beweisen Sie, dass Sie kein Roboter sind, und lösen Sie die folgende Rechenaufgabe: nur beim Absenden ohne Konto (nur für belgische Unternehmen, die über die KBO-Nummer registriert sind).