Gegevensbeschermingsautoriteit

Velden melding gegevensinbreuk DEEL 1

Contents

1. Informatie

Informatie over de verwerking van persoonsgegevens

De Gegevensbeschermingsautoriteit verwerkt uw persoonsgegevens omdat zij wettelijk verplicht is om gegevensinbreuken te registeren, voor handhaving en controle en indien nodig advies te geven aan de organisatie over de gegevensinbreuk. De persoonsgegevens worden bewaard zolang dit nodig is in het kader van advisering, handhaving en controle en dit tot 10 jaar na afsluiten dossier (bij rechtsvordering tot het einde van de procedure). In het kader van de samenwerking met andere Europese en/of nationale gegevensbeschermingsautoriteiten kunnen gegevens uit dit formulier met hen worden gedeeld.

Voor meer informatie of voor het uitoefenen van uw gegevensbeschermingsrechten, zie onze privacyverklaring.

Dit meldingsformulier betreft een melding van een gegevensinbreuk aan de Gegevensbeschermingsautoriteit conform artikel 33 AVG.

Wanneer het gaat om een gegevensinbreuk die eveneens onder het toepassingsgebied van de Wet Elektronische Communicatie valt en wanneer de verwerkingsverantwoordelijke een operator van elektronische communicatiediensten betreft die werd aangemeld bij het BIPT, wordt een kopie van deze melding overgemaakt aan het BIPT, dit overeenkomstig art. 107/3, §2 WEC.

De verantwoordelijke voor de verwerking stelt de Gegevensbeschermingsautoriteit waar uiterlijk 72 uur na kennisname in kennis van een gegevensinbreuk.

Vrije tekstvelden hebben een maximum van 100 tekens (inclusief spaties), tenzij anders vermeld.

Om de gegevensinbreuk vlot in te dienen heeft u (mogelijk) volgende informatie nodig bij het meldproces

- Indien van toepassing: Contactgegevens en referentie actieve DPO-case van de aanmelding van uw DPO
- Correspondentie over de ontdekking van de gegevensinbreuk
- Indien van toepassing: verwerkingsregister (artikel 30 AVG)
- Gegevensinbreukregister (artikel 33.5 AVG)
- De maatregelen die reeds in voege waren voor de gegevensinbreuk
- De maatregelen die werden genomen om de gegevensinbreuk te beëindigen
- De maatregelen die werden genomen of zijn vooropgesteld om de gegevensinbreuk in de toekomst te voorkomen
- Indien van toepassing: advies van de DPO
- De Gegevensbeschermingseffectbeoordeling (GEB) (art. 35 AVG) (indien van toepassing)
- Indien van toepassing: De mededeling van de gegevensinbreuk aan de betrokkene(n) (art. 34 AVG)

Indien er sprake is geweest van een hacking (in de meest brede zin), phishing of een andere (cyber)incident waarbij een (extern) onderzoek heeft plaatsgevonden:

- Het onderzoeksrapport naar aanleiding van de gegevensinbreuk

Als u samenwerkt met een verwerker of wanneer de gegevensinbreuk plaatsvond bij een derde partij:

- De verwerkersovereenkomst (art. 28 AVG)
- Protocolakkoorden tussen overheden (art. 20 Kaderwet)
- Andere overeenkomsten, zoals een samenwerkingsovereenkomst (art. 26 AVG)

Als u een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker bent:

- De vertegenwoordigersovereenkomst (art. 27 AVG);

Onderzoek bij *hacking* (in de meest brede zin), *phishing* of een andere cyberincident waarbij persoonsgegevens geïmpacteerd werden

Wanneer u een gegevensinbreuk meldt aan de Gegevensbeschermingsautoriteit ten gevolge van *hacking* (in de meest brede zin), *phishing* of een andere (cyber)incident waarbij persoonsgegevens geïmpacteerd werden, verwachten wij dat u zo snel mogelijk onderzoek doet of laat doen naar de omvang van het incident. Dit onderzoek is noodzakelijk om er voor te zorgen dat:

- Er geen *backdoors* en andere kwaadwillige bestanden in het systeem aanwezig blijven
- Om duidelijkheid te krijgen over de vraag of persoonsgegevens door derden zijn ingezien, gekopieerd, gestolen of gewijzigd.

De Gegevensbeschermingsautoriteit verwacht dat u volgende vragen in uw onderzoek betrekt:

- Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox, tot printopdrachten op een *printserver*, tot de inhoud van een database, tot bestanden op een *fileserver* waar persoonsgegevens in worden verwerkt, …
- Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers? Werd er een *flow* gedetecteerd (al dan niet via de firewall) van informatie naar een omgeving buiten de onderneming?
- Zijn er loggegevens beschikbaar en zo ja, is het mogelijk om met deze loggegevens uit te sluiten dat persoonsgegevens zijn gekopieerd of ingezien?

Documentatieplicht- gegevensinbreukregister:

Het melden van een gegevensinbreuk die een mogelijk risico inhoudt voor de rechten en vrijheden van natuurlijke personen aan de Gegevensbeschermingsautoriteit vormt een onderdeel van de verplichtingen inzake gegevensinbreuken. Verwerkingsverantwoordelijken zijn eveneens verplicht om deze intern te registeren in het gegevensinbreukregister. Deze documentatieplicht geldt overigens voor alle gegevensinbreuken, dus ook voor deze die geen risico inhouden voor de rechten en vrijheden van natuurlijke personen. Overeenkomstig art. 33.5 AVG dient minstens volgende informatie te worden opgenomen:

- De feiten over de gegevensinbreuk, zoals de oorzaak, wat er precies is gebeurd, wanneer precies welke stappen zijn ondernomen en om welke persoonsgegevens het gaat;

- De gevolgen van de gegevensinbreuk;
- De maatregelen die werden genomen om de gegevensinbreuk te beëindigen en om herhaling te voorkomen;

Melding van gegevensinbreuk waarbij verschillende risiconiveaus ten aanzien van verschillende betrokkenen aanwezig zijn
Indien u een gegevensinbreuk meldt waaruit verschillende risiconiveaus volgen ten aanzien van verschillende betrokkenen die voortvloeien uit eenzelfde incident, dient u in uw melding de hoogste risiconiveaus op te nemen.

Verificatie: enkel bij indienen zonder account (enkel voor Belgische ondernemingen die via KBO-nummer kunnen aanloggen – FAS)

Ondernemingsnummer*

Reeds ingevuld op basis van input inlogflow

Land*

Reeds ingevuld: België

2. Introductie

Op grond van welke regelgeving meldt u?*

☐ Algemene verordening gegevensbescherming (AVG) – art. 33 AVG
☐ Wet Elektronische Communicatie (WEC) – art 107/3, §3 WEC
☐ Wetboek Economisch Recht (WER) – art. XII.27 WER

Indien u onder de NIS(II) valt dient u ook een melding te verrichten bij het CCB via volgende link: https://notif.safeonweb.be/nl

Indien u een financiële dienstverlener bent dient u mogelijks ook een melding te verrichten bij de NBB onder PSDII via volgende link: https://www.nbb.be/en/onegate

3. Organisatie

3.1. Contactgegevens van de verwerkingsverantwoordelijke

3.2. Naam van de organisatie*

vrij tekstveld

3.3. Hoofdvestiging*

- In België (go to 3.3.1.)
- In EU/EEA land (go to 3.3.2 and 3.3.3.)
- Buiten EU/EEA (go to 3.3.2 and 3.3.4.)

3.3.1. Ondernemingsnummer*

Reeds ingevuld op basis van inlogflow of ingevuld op basis van ondernemingsaccount

3.3.2. Land van hoofdvestiging*

Drop down: landenlijst – één keuze mogelijk

3.3.3. Europees BTW-nummer*

Gestructureerd tekstveld

3.3.4. Uniek Landnummer*

vrij tekstveld

3.4. In welke sector is de verwerkingsverantwoordelijke actief?*

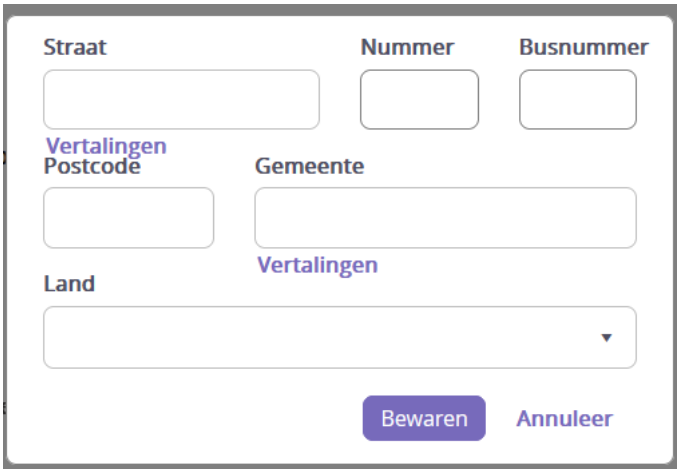
Drop down keuzelijst sector – verschillende antwoorden mogelijk :
Administratieve en ondersteunende diensten
Andere (go to 3.4.1.)
Arbeid(sbemiddeling), uitzendbureaus en personeelbeheer
Bouwnijverheid
Exploitatie van en handel in onroerend goed
Extraterritoriale organisaties en instanties
Financiele activiteiten en verzekeringen
Groot- en detailhandel
Horeca
Industrie
Informatie en communicatie
Kunst, cultuur, amusement en recreatie
Menselijke gezondheidszorg en maatschappelijke dienstverlening
Nutsbedrijven
Onderwijs
Openbaar bestuur
Overige diensten
Overige organisatie – levensbeschouwelijke organisaties
Overige organisatie – politieke organisaties
Overige organisatie – vakbonden
Overige zakelijke dienstverlening – accountancy, belastingadvisering en administratie
Overige zakelijke dienstverlening – wetenschappelijk onderzoek
Politie en justitie
Sociale netwerken (bedrijven)
Vervoer
Vrije beroepen en wetenschappelijke en technische activiteiten

3.4.1. Andere sector*

Vrij tekst veld

3.5. Adresgegevens en contactgegevens van de verwerkingsverantwoordelijke* (?)

(?) Hebt u hulp nodig? Informatie adres: Enkel Belgische adressen worden automatisch ingevuld. Andere adressen kunnen zonder probleem handmatig worden ingevoerd, waarbij het voorgestelde adres genegeerd of overschreven kan worden.



3.6. E-mail verwerkingsverantwoordelijke* (?)

(?) Hebt u hulp nodig? E-mail Verwerkingsverantwoordelijke: Gelieve hier een algemeen e-mailadres voor de onderneming te willen invullen en geen persoonlijk e-mailadres of een e-mailadres dat direct identificeerbare persoonsgegevens bevat.

Vrij tekst veld

3.7. Is de verwerkingsverantwoordelijke een (telecom)operator die aangemeld is bij het BIPT?* (?)

(?) hebt u hulp nodig? BIPT: https://www.bipt.be/operatoren/publication/lijst-van-telecomoperatoren

Dropdown:
ja
nee

3.8. Is de verwerkingsverantwoordelijke een beursgenoteerde onderneming?*

Dropdown:
ja
nee

3.9. Vond de gegevensinbreuk plaats in een verwerking die is uitbesteed aan een verwerker?*

Dropdown:
Ja (go to 2.9.1.)
nee

3.9.1. Over welke verwerker gaat het?*

Toevoegen: (meerdere mogelijk)

3.10. Contactpersoon voor de Gegevensinbreuk

Naam persoon*

Vrij tekstveld

Voornaam persoon*

Vrij tekstveld

Functie contactpersoon

Vrij tekstveld

Telefoonnummer contactpersoon*

Gestructureerd tekstveld

E-mail contactpersoon*

Gestructureerd tekstveld

4. Internationaal

4.1. Grensoverschrijdende inbreuk

4.1.1. Heeft de inbreuk gevolgen voor betrokkenen in meerdere landen?*

Dropdown:
Ja (go to 4.1.2 en 4.2.1.)
Nee

4.1.2. Als er sprake is van een grensoverschrijdende verwerking, over welke landen (inclusief België indien van toepassing) gaat het en om hoeveel betrokkenen gaat het binnen deze landen (?)*

(?) Hebt u hulp nodig? Gelieve hieronder de verschillende landen en het aantal personen voor deze landen aan te geven waarvoor de grensoverschrijdende gegevensinbreuk gevolgen heeft. Indien het niet mogelijk zou zijn om het exacte aantal personen te identificeren, gelieve deze bij benadering aan te duiden.

Toevoegen: (meerdere mogelijk)

Land	Betrokkenen
Keuzelijst landen	*Aantal betrokkenen*

4.2. Bevoegde toezichthouders in andere EU-lidstaten

4.2.1. Heeft uw organisatie de inbreuk gemeld bij andere gegevensbeschermingsautoriteiten?*

Dropdown:
Ja (go to 4.2.1.1.)
nee

4.2.1.1. Gelieve aan te geven in welke landen u de inbreuk aan de Gegevensbeschermingsautoriteiten heeft gemeld*

Toevoegen: (meerdere mogelijk)

Keuzelijst: landen

5. Tijdslijn

5.1. Datum en uur waarop de gegevensinbreuk zich heeft voorgedaan*

Wanneer heeft de gegevensinbreuk zich voorgedaan?*

Dropdown:
Niet gekend
Exacte datum en tijd waarop de gegevensinbreuk plaatsvond is gekend, namelijk: (go to 5.1.1.)
Exacte datum en tijd waarop de gegevensinbreuk plaatvond is niet gekend, maar wordt geschat op: (go to 5.1.1.)

5.1.1. Datum en uur waarop de gegevensinbreuk zich heeft voorgedaan*

Datumveld: kalender	*Tijdsveld: tijd*

5.2. Datum en uur van ontdekking van de gegevensinbreuk*

Wanneer werd de gegevensinbreuk ontdekt?*(?)

(?) Hebt u hulp nodig? GI - Datum en tijd ontdekking GI: Het moment van ontdekking van een gegevensinbreuk is niet hetzelfde als het moment waarop het incident aan de DPO wordt gemeld. De DPO is niet verantwoordelijk voor de meldplicht aan een Toezichthoudende Autoriteit. De Gegevensbeschermingsautoriteit accepteert het moment van melding aan de DPO dan ook niet als rechtvaardiging voor een te late melding.

Datumveld: kalender (go to 5.3 indien van toepassing)	*Tijdsveld: tijd (go to 5.3 indien van toepassing)*

5.3. Rechtvaardiging voor het laattijdig melden van de gegevensinbreuk aan de Gegevensbeschermingsautoriteit*

Als deze melding niet binnen de 72 uur na het ontdekken van de gegevensinbreuk wordt verricht, wat is de reden hiervoor? Vrij tekstveld – (AVG)

Als deze melding niet binnen de 24 uur na het ontdekken van de gegevensinbreuk wordt verricht, wat is de reden hiervoor? Vrij tekstveld – (WEC /WER)

5.4. Wanneer werd de gegevensinbreuk verholpen?*

Dropdown:
De gegevensinbreuk is nog niet verholpen (go to 5.4.1.)
De gegevensinbreuk is verholpen (go to 5.4.2.)

5.4.1. De reden hiervoor is:*

Vrij tekstveld

5.4.2. Wanneer werd de gegevensinbreuk verholpen?*

Datumveld: kalender	*Tijdsveld: tijd*

6. Verwerking

6.1. Doelen waarvoor de persoonsgegevens worden verwerkt*

Vrij tekstveld

6.2. Aard van de persoonsgegevens die getroffen zijn door de gegevensinbreuk*

Persoonsgegevens in het algemeen

- ☐ Identificatiegegevens (bijvoorbeeld naam, adres, geboortedatum, telefoonnummer, nummerplaat, klantnummer,…)
- ☐ Elektronische identificatiegegevens (bijvoorbeeld e-mailadressen, IP-adressen,…)
- ☐ Persoonlijke kenmerken (bijvoorbeeld leeftijd, geslacht, burgerlijke staat,…)
- ☐ Fysieke gegevens (bijvoorbeeld grootte, gewicht, uiterlijk,…)
- ☐ Samenstelling van het gezin
- ☐ Vrijetijdsbesteding en interesses
- ☐ Sociaal mediaprofiel
- ☐ Lidmaatschappen
- ☐ CRM data (bijvoorbeeld informatie over klanten, contacten, communicatie, tevredenheid,…)
- ☐ (Klant)profielen (bijvoorbeeld voorspelling van een bepaald kenmerk of gedrag,…)
- ☐ Leef-, klik-, mail-, zoek-, surf-, betaal- en/of consumptiegewoonten
- ☐ Product en dienstverlening (onkosten, verbruik, onderhoud,…)
- ☐ Woning-, autokenmerken
- ☐ Foto's of beeldopnamen (bijvoorbeeld cctv, bewakingscamera, opgenomen opleiding,…)
- ☐ Geluidsdopnamen (bijvoorbeeld opgenomen telefoongesprekken van call center, -klantendienst,…)
- ☐ Opleiding en vorming
- ☐ Beroep en betrekking, BTW-regime
- ☐ HR data (data aangaande salaris en personeelsaanwezigheid evaluaties, KPI, carrièreplanning,…)
- ☐ Fysieke en/of ICT beveiligingsgegevens van klanten, personeel en bezoekers (bijvoorbeeld toelatingen en rechten, gebruik van badge, internettoegang,…)

- ☐ Gegevens m.b.t. controle op klanten of personeel (bijvoorbeeld logging, klokkenluidersregeling, klachtenafhandeling, kwaliteitscontrole, …)
- ☐ Andere: *(vrij tekstveld)*

Uniek identificatienummer

- ☐ Nationaal nummer (bijvoorbeeld het Rijksregisternummer)
- ☐ Identificatienummer van de sociale zekerheid
- ☐ Andere: *(vrij tekstveld)*

Bijzondere categorieën van persoonsgegevens (artikel 9.1 AVG)

- ☐ Raciale of etnische afkomst
- ☐ Politieke opvattingen
- ☐ Religieuze of levensbeschouwelijke overtuigingen
- ☐ Lidmaatschap van een vakbond
- ☐ Genetische gegevens (bijvoorbeeld DNA, bloedgroep,…)
- ☐ Biometrische gegevens (bijvoorbeeld vingerafdruk, irisscan,…)
- ☐ Gegevens over gezondheid
    - ☐ Fysieke gegevens
    - ☐ Psychische gegevens
    - ☐ Gegevens met betrekking tot zorg
    - ☐ Andere: *(vrij tekstveld)*
- ☐ Gegevens over seksueel gedrag of seksuele geaardheid

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 10 AVG)

- ☐ Strafrechtelijke veroordelingen
- ☐ Strafbare feiten
- ☐ Veiligheidsmaatregelen die betrekking hebben op strafrechtelijke veroordelingen of strafbare feiten
- ☐ Uittreksel uit het strafregister

Persoonsgegevens buiten de artikelen 9.1. en 10 AVG die als gevoelig worden behandeld omdat hun verwerking een bepaald risico kan inhouden voor de rechten en vrijheden van de betrokkenen zoals :

- ☐ Inhoud van de elektronische communicatiegegevens
- ☐ Smart Grid (bijvoorbeeld slimme meters,…)
- ☐ Locatiegegevens in brede zin (bijvoorbeeld al dan niet verwerkt door telecomoperatoren of via navigatiesoftware, GPS,…)
- ☐ Financiële gegevens (bankkaartnummer, rekeningnummer, verzekeringspolisnummer, salaris en inkomen,…)
- ☐ Toegangscode (wachtwoord, PIN-code,…)
- ☐ Kopieën van paspoort, e-ID of andere legitimatiebewijzen
- ☐ Andere: *(vrij tekstveld)*

6.3. Aantal betrokkenen van wie persoonsgegevens werden getroffen*

6.3.1. Is het exacte aantal betrokkenen bekend?*

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

6.3.1.1. Aantal Personen/Betrokkenen*

Aantal/cijfer

6.3.1.2. Minimaal/maximaal aantal Personen/Betrokkenen*

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de gegevensinbreuk (als slachtoffer)?	Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de gegevensinbreuk (als slachtoffer)?
Aantal/cijfer	*Aantal/cijfer*

7. Oorzaak

Wat is de oorzaak van de gegevensinbreuk?

7.1. Type gegevensinbreuk* (?)

(?) Hebt u hulp nodig? Type gegevensinbreuk: Voor meer informatie omtrent de verschillende types gegevensinbreuken in dit formulier, bekijk onze handleiding voor gegevensinbreuken op de website van de Gegevensbeschermingsautoriteit.

- ☐ E-mail met persoonsgegevens verstuurd naar verkeerde ontvangers
- ☐ E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in cc, in plaats van bcc
- ☐ Brief of pakket met persoonsgegevens werd verstuurd of afgegeven aan de verkeerde ontvanger
- ☐ Autorisaties van interne of externe medewerkers verkeerd ingesteld (autorisaties ten aanzien van persoon) (?)
  (?) Hebt u hulp nodig? De gegevensinbreuk heeft betrekking op een situatie waarbij de toegangs- of leesrechten van een gebruiker niet of kwaadwillig foutief of kwaadwillig zijn aangepast, waardoor een gebruiker meer mogelijkheden heeft in het systeem dan zou moeten. Bijvoorbeeld: bij functiewijziging werd een autorisatierol niet goed doorgevoerd; te uitgebreide ingestelde toegangsrechten; adminrights voor niet-geautoriseerde personen; etc.
- ☐ Netwerkmappen, applicaties of – locatie met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie (autorisaties ten aanzien van bestand) (?)
  (?) Hebt u hulp nodig? De gegevensinbreuk heeft betrekking op een situatie waarbij een (gedeelde) map, locatie of applicatie binnen de organisatie verkeerd is ingesteld en daardoor voor interne onbevoegde personen is te zien. Bijvoorbeeld: een map met personeelsgegevens die voorbehouden is voor de HR-afdeling was toegankelijk voor elke medewerker.
- ☐ Netwerkmappen, -applicaties of – locatie met persoonsgegevens toegankelijk van buiten de organisatie (?)
  (?) Hebt u hulp nodig? De gegevensinbreuk heeft betrekking op een situatie waarbij een bestand, locatie of applicatie connectie heeft met het internet en deze voor onbevoegden toegankelijk is via het internet. Bijvoorbeeld extranet van een organisatie is toegankelijk voor onbevoegden buiten de organisatie.
- ☐ Apparaat (mobiel, tabblad, etc.), gegevensdrager (bijv. USB-stick)en/of papier met persoonsgegevens verloren
- ☐ Apparaat (mobiel, tabblad, etc.), gegevensdrager (bijv. USB-stick)en/of papier met persoonsgegevens gestolen
- ☐ Persoonsgegevens onterecht gepubliceerd. (Bijvoorbeeld indexatie in zoekmachine; gegevens gepubliceerd op een website, op een sociaal media platform, op een papieren drager (krant, tijdschrift, etc.)) (?)
  (?) Hebt u hulp nodig? De gegevensinbreuk heeft betrekking op een situatie waarbij

(een bestand met) persoonsgegevens per ongeluk werden gepubliceerd. Bijvoorbeeld indexatie van dossier in zoekmachines, publicatie van niet-gepseudonimiseerde beslissingen, ongewilde publicatie van persoonsgegevens op social media platforms, etc.

- ☐ Persoonsgegevens van verkeerde persoon getoond in persoonlijk portaal of soortgelijke omgeving
- ☐ Persoonsgegevens niet (correct) vernietigd (bijvoorbeeld leesbare persoonsgegevens bij oud papier gezet)
- ☐ Persoonsgegevens onterecht vernietigd
- ☐ DNS-spoofing/poisoning (?)
  (?) hebt u hulp nodig? DNS-spoofing, ook wel cache poisoning genaamd, betreft een gegevensinbreuk waarbij een browser wordt gemanipuleerd zodat bezoekers van een website worden omgeleid naar kwaadaardige websites die erop uit zijn om gevoelige informatie te stelen. DNS-spoofing vindt plaats wanneer uw cache wordt besmet met deze kwaadaardige omleidingen.
- ☐ Phishing
- ☐ Ransomware
- ☐ Credential Stuffing (?)
  (?) hebt u hulp nodig? Credential stuffing is het automatisch invoeren van gestolen gebruikersnamen en wachtwoorden ("inloggegevens") in inlogformulieren van websites om op frauduleuze wijze toegang te krijgen tot gebruikersaccounts.
- ☐ SQL-Injection (?)
  (?) hebt u hulp nodig? SQL-injectie (SQLi) is een kwetsbaarheid in de webbeveiliging waardoor een aanvaller de query's kan verstoren die een applicatie naar zijn database stuurt. Hierdoor kan een aanvaller gegevens bekijken die hij normaal gesproken niet kan ophalen. Dit kunnen gegevens zijn die aan andere gebruikers toebehoren, of andere gegevens waartoe de applicatie toegang heeft. In veel gevallen kan een aanvaller deze gegevens wijzigen of verwijderen, waardoor de inhoud of het gedrag van de applicatie blijvend wordt gewijzigd.
- ☐ (D)DOS-attack (?)
  (?) hebt u hulp nodig? Een distributed denial-of-service (DDoS)-aanval is een kwaadwillige poging om het normale verkeer van een bepaalde server, dienst of netwerk te verstoren door het doelwit of de omliggende infrastructuur te overspoelen met een stortvloed aan internetverkeer.
- ☐ AI-models (leakage/regurgitation,…) (?)
  (?) hebt u hulp nodig? Regurgitatie is het fenomeen waarbij een AI-model reacties genereert die dicht bij de trainingsgegevens liggen, waardoor mogelijk gevoelige informatie wordt onthuld.
- ☐ Coordinated Vulnerability Disclosure Policy/Bug-bounty (?)
  (?) hebt u hulp nodig? Een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden (of in het Engels "Coordinated Vulnerability Disclosure Policy" - CVDP) is een geheel van regels die vooraf zijn bepaald door een organisatie die verantwoordelijk is voor informatiesystemen waardoor deelnemers (of "ethische hackers") met goede bedoelingen mogelijke kwetsbaarheden in haar systemen kunnen opsporen, of haar alle relevante informatie hierover kunnen bezorgen. Een beloningsprogramma voor het opsporen van kwetsbaarheden (of in het Engels "bug bounty") heeft betrekking op alle regels die een verantwoordelijke organisatie heeft bepaald om beloningen toe te kennen aan deelnemers die kwetsbaarheden identificeren in de door haar gebruikte technologieën. Het betreft een beleidsvorm voor de gecoördineerde bekendmaking van kwetsbaarheden die voorziet in de toekenning van een beloning aan de deelnemer naargelang de hoeveelheid, het belang of de kwaliteit van de bezorgde informatie.

□ Andere: *vrij tekstveld*

7.2. Samenvatting van de gegevensinbreuk* (?)

(?) Hebt u hulp nodig? Samenvatting van de geevensinbreuk: Geef bij het samenvatten van de gegevensinbreuk meer informatie over:

- *De oorzaak, aard, type en de omstandigheden van de gegevensinbreuk*
- *Het tijdstip en de ontdekking van de gegevensinbreuk*
- *Omschrijving van de (getroffen) verwerking en getroffen persoonsgegevens*
- *De genomen acties en beslissingen (tijdslijn) tot op heden*

Vrij teksteveld – maximum 2500 tekens

8. Mededeling (?)

(?) Hebt u hulp nodig? Informatiestrekking: Melding aan betrokkenen bij gegevensinbreuk:

De GBA adviseert melding aan betrokkenen bij gegevensinbreuken die betrekking hebben op:

- *Bijzondere categorieën persoonsgegevens (art. 9.1 AVG).*
- *Strafrechtelijke gegevens (art. 10 AVG).*
- *Kopieën van identiteitsbewijzen/paspoorten of rijksregisternummers.*
- *Gegevens van kwetsbare groepen (bv. minderjarigen).*
- *Grote hoeveelheden gegevens of een groot aantal betrokkenen.*

En kan leiden tot:

- *Discriminatie, identiteitsfraude, financiële verliezen, of reputatieschade.*
- *Schending van privacy, beroepsgeheim, of aanzienlijke impact op rechten en vrijheden.*

Aanbevelingen GBA (art. 34 AVG):

- *Als de individuele contactgegevens van betrokkenen beschikbaar zijn, dient in principe een individuele mededeling plaats te vinden - los van het aantal betrokkenen.*
- *Een openbare melding, zoals een banner op de website, dient even doeltreffend te zijn als een individuele mededeling.*
- *Maatregelen ter voorkoming van toekomstige inbreuken zijn niet voldoende; alleen acties die risico's van de huidige inbreuk beperken zijn geldig om aanspraak te maken op de uitzonderingsgrond in art. 34 AVG.*

Inhoud van de melding: De melding dient best:

- *Specifieke categorieën van getroffen gegevens benoemen om betrokkenen te informeren over risico's.*
- *Voorstellen bevatten voor maatregelen die betrokkenen zelf kunnen nemen.*

Phishing-incidenten: Bij phishing moeten mogelijk drie groepen geïnformeerd worden:

- *De personen die phishingmails hebben ontvangen en de eigenaar van de gehackte mailbox.*
- *Personen van wie gegevens in e-mails of bijlagen staan van de gehackt mailbox.*

8.1. Heeft u de inbreuk reeds gemeld aan de betrokkenen?*

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

8.1.1. Heeft u de betrokkenen individueel ingelicht?*

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

8.1.1.1. Welk communicatiemiddel of -kanaal heeft u gebruikt om de betrokkenen individueel te informeren?*

☐ Telefonisch ☐ Per brief ☐ Per e-mail ☐ Ander kanaal: *(vrij tekstveld)*

8.1.1.2. Aan hoeveel betrokkenen heeft u de gegevensinbreuk individueel gemeld?*

aantal

8.1.1.3. Wanneer heeft u de gegevensinbreuk individueel gemeld aan de betrokkenen?*

Datumveld: kalender

8.1.1.4. Welk communicatiemiddel of -kanaal heeft u gebruikt om de betrokkenen collectief te informeren?*

☐ Via een mededeling op de website ☐ Via sociale media ☐ Via een advertentie in de krant ☐ Ander kanaal: *(vrij tekstveld)*

8.1.1.5. Wanneer heeft u de gegevensinbreuk collectief gemeld aan de betrokkenen?*

Datumveld: kalender

8.2. Gaat u de inbreuk nog melden aan de betrokkenen?*

Dropdown:
Ja (go to 8.2.1; 8.2.2.)
Nee
Nog niet bekend

8.2.1. Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkenen?*

Datum veld: Kalender

8.2.2. Gaat u de betrokkenen individueel inlichten?*

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

8.2.2.1. Welk communicatiemiddel of -kanaal gaat u gebruiken om de betrokkenen individueel te informeren?*

☐ Telefonisch ☐ Per brief ☐ Per e-mail ☐ Ander kanaal: *(vrij tekstveld)*

8.2.2.2. Aan hoeveel betrokkenen gaat u de gegevensinbreuk melden?*

Cijfer/aantal

8.2.2.3. Welk communicatiemiddel of -kanaal heeft u gebruikt om de betrokkenen collectief te informeren?*

☐ Via een mededeling op de website ☐ Via sociale media ☐ Via een advertentie in de krant ☐ Ander kanaal: *(vrij tekstveld)*

8.2.2.4. Aan hoeveel betrokkenen gaat u de gegevensinbreuk melden?*

Cijfer/aantal

9. Bijkomend

Geef hier elke informatie aan die de melding beter kan doen begrijpen. (*Maximum 2000 tekens)*

Verklaring

☐ Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

Bewijs dat u geen robot bent en los volgende som op: enkel bij indienen zonder account (enkel voor Belgische ondernemingen die via KBO-nummer