Gegevensbeschermingsautoriteit

Velden melding gegevensinbreuk DEEL 2

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.

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

2.1. Heeft u de gegevensinbreuk eveneens gemeld bij andere nationale toezichthouders op basis van andere meldplichten; of klacht neergelegd bij de politie en/of parket? Of gaat u dat nog doen en bij welke?

Dropdown:
Ja (go to 2.1.1.)
nee

2.1.1. Lijst toezichthouders

☐ Centrum voor Cybersecurity Belgium (CCB) – Cyber Emergency Response Team (CERT)

*Ref. CCB**

☐ Nationale Bank van België (NBB)

*Ref. BNB**

☐ FOD economie

*Ref. FOD Economie**

☐ Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT)

*Ref. BIPT**

☐ (Lokale of federale) Politie en/of Parket

*PV nummer**

☐ Andere toezichthouder

*Andere Toezichthouder**	*Referentie andere Toezichthouder**

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?*

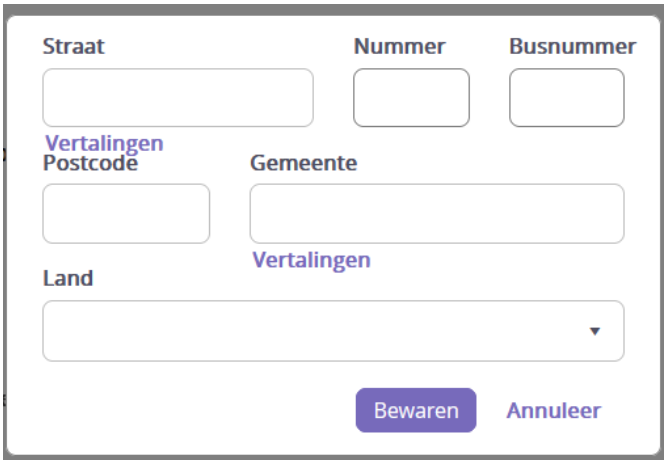
Drop down keuzelijst sector – verschillende antwoorden mogelijk :
Administratieve en ondersteunende diensten
Andere (go to 3.4.1.)
Arbeid(sbemiddeling), uitzendbureaus en personeelbeheer
Bouwnijverheid
Exploitatie van en handel in onroerend goed
Extraterritoriale organisaties en instanties
Financiele 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?*

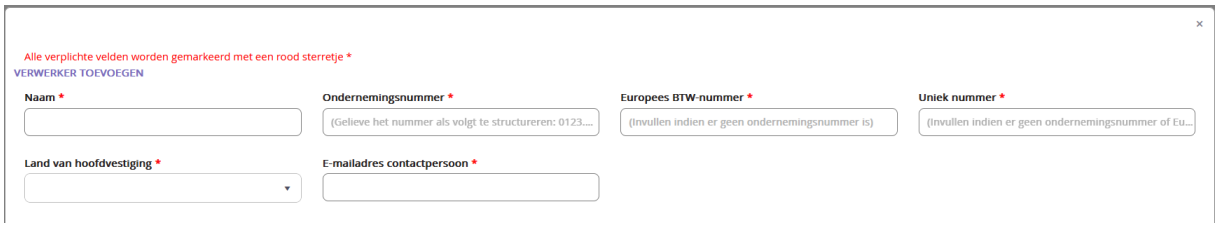
Dropdown:
ja
nee

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

3.11. Beschikt de verwerkingsverantwoordelijke over een DPO?*

Dropdown:
Ja (go to 3.11.1)
nee

3.11.1. DPO-Case*

Selecteer

Indien u uw DPO nog niet heeft aangemeld, gelieve dit eerst te doen via het portaal

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*

4.1.3. Bevindt de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke in België?*

Dropdown:
Ja
nee

4.1.4. Wordt de melding gemaakt op basis van one-stop-shop?*(?)

(?) Hebt u hulp nodig? One-stop-shop: One-stop-shop is het mechanisme waarbij één toezichthoudende autoriteit fungeert als leidende toezichthoudende autoriteit voor verwerkingsverantwoordelijken met meerdere vestigingen in de Europese Economische Ruimte. In dit geval is de leidende toezichthoudende autoriteit de toezichthoudende autoriteit van de lidstaat waar de hoofdvestiging van de verwerkingsverantwoordelijke zich bevindt. Bij het melden van gegevensinbreuken met grensoverschrijdende effecten kan de verwerkingsverantwoordelijke, met meerdere vestigingen in de EER, gebruik maken van het one-stop-shop-mechanisme door de gegevensinbreuk (enkel) te melden aan de toezichthoudende autoriteit waar haar hoofdvestiging zich bevindt.

Dropdown:
Ja
nee

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

4.2.2. Zal de gegevensinbreuk nog worden gemeld bij andere Gegevensbeschermingsautoriteiten?*

Dropdown:
Ja (go to 4.2.2.1.)
nee

4.2.2.1. Gelieve aan te geven in welke landen u de gegevensinbreuk aan de Gegevensbeschermingsautoriteiten nog zult melden*

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 5.4 indien van toepassing)	*Tijdsveld: tijd (go to 5.4 indien van toepassing)*

5.3. Wijze waarop de gegevensinbreuk is ontdekt*

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

5.3.1. Interne melding

Keuzelijst: verschillende antwoorden mogelijk

- ☐ Van verlies van hardware
- ☐ Beheersproces (bv. ICT incident meldingssysteem, informatieveiligheid incident management,…)
- ☐ Cyber emergency team procedure
- ☐ Controlesysteem om indringen of inbreuken te detecteren en ongeoorloofde toegang op te sporen
- ☐ Controleprocedure/klokkenluidersregeling
- ☐ Klachtenafhandelingsdienst
- ☐ Andere: *(vrij tekstveld: gelieve naam en tijdstip mee te delen*)*

5.3.2. Externe melding

Keuzelijst: verschillende antwoorden mogelijk

- ☐ Door een leverancier, onderaannemer of verwerker (go to 5.3.2.1.)
- ☐ Door een klant (go to 5.3.2.1.)
- ☐ Door een derde (go to 5.3.2.1.)
- ☐ Door een ethische hacker
- ☐ Door een autoriteit (go to 5.3.2.1.)

5.3.2.1. Indien externe melding door een leverancier, onderaannemer, verwerker , klant, derde of autoriteit*

Vrij tekstveld: gelieve naam en tijdstip mee te delen

5.4. 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)

5.5. 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.)

5.5.1. De reden hiervoor is:*

Vrij tekstveld

5.5.2. 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 *(keuzelijst: verschillende antwoorden mogelijk)*

- ☐ 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 *(keuzelijst: verschillende antwoorden mogelijk)*

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

Bijzondere categorieën van persoonsgegevens (artikel 9.1 AVG) *(keuzelijst: verschillende antwoorden mogelijk)*

- ☐ 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) *(keuzelijst: verschillende antwoorden mogelijk)*

☐ 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 *(keuzelijst: verschillende antwoorden mogelijk)*

☐ 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*

6.4. Groepen van betrokkenen die getroffen zijn door de gegevensinbreuk*

Meerdere antwoorden mogelijk

☐ Burgers
☐ Consumenten
☐ Gebruikers
☐ Gevangenen

- ☐ Leveranciers
- ☐ Kinderen
- ☐ Militairen of leden van de politie
- ☐ Ouderen
- ☐ Patiënten
- ☐ Leerlingen en/of studenten
- ☐ Vluchtelingen en asielzoekers
- ☐ Werknemers/medewerkers (kandidaten)
- ☐ Andere *(vrij tekstveld: Andere, namelijk:*)*
- ☐ Niet gekend

6.5. De graad en mogelijkheid van identificatie van de betrokkenen o.b.v. de onderliggende gegevens* (?)

(?) Hebt u hulp nodig? Graad van identificatie van de betrokkene(n): Direct identificeerbare gegevens - Gegevens waaruit voor derden de identiteit van de betrokkenen direct blijkt.

Indirect en makkelijk identificeerbare gegevens - Gegevens waaruit de identiteit van de betrokkenen niet direct blijkt, maar die door derden vrij eenvoudig gelinked kunnen worden aan (publiek) toegankelijke identificatiegegevens van de betrokkenen.

Indirect identificeerbare gegevens - Gegevens waaruit niet elke derde direct de identiteit van de betrokkene kan achterhalen. Er zijn evenwel methodes voorhanden om met behulp van aanvullende (niet-publieke) data toch de burgerlijke identiteit van de betrokkene te achterhalen.

Indirect tot betrokkenen herleidbare gegevens - Er bestaan technieken en methodes die derden toelaten om (een deel van) de dataset te herleiden tot specifieke individuen (zgn. afzonderen van personen in datasets of "single out").

Meerdere antwoorden mogelijk

- ☐ Direct identificeerbare gegevens
- ☐ Indirect en makkelijk identificeerbare gegevens
- ☐ Indirect identificeerbare gegevens
- ☐ Indirect tot betrokken herleidbare gegevens

7. Oorzaak

7.1. Wat is de oorzaak van de gegevensinbreuk?

De oorzaak van de gegevensinbreuk lag*

Dropdown:
Intern (bijvoorbeeld door personeel)
Extern (bijvoorbeeld door een hacker)

De gegevensinbreuk werd veroorzaakt door*

Dropdown:
Systeemtechnisch handelen
Menselijk handelen

De intentie rond de gegevensinbreuk was*

Dropdown:
Accidenteel
Kwaad opzet

7.2. Wat is de aard van de gegevensinbreuk?

☐ Inbreuk op het vertrouwelijk karakter van de persoonlijke gegevens – confidentialiteitsinbreuk (go to 7.2.1.)
☐ Inbreuk op de beschikbaarheid van de persoonlijke gegevens – beschikbaarheidsinbreuk (go to 7.2.2.)
☐ Inbreuk op de integriteit van de persoonlijke gegevens – integriteitsinbreuk (go to 7.2.3.)

7.2.1. Distributie – grootorde van ontvangers van de gegevens* (?)

(?) Hebt u hulp nodig? Aantal Personen :

- *Beperkte groep: Kleiner dan 10% van het aantal medewerkers.*
- *Grote groep: Vanaf 10% van het aantal medewerkers.*

Bolean: één mogelijkheid

- Ongekend aantal personen
- Gekend aantal personen:
  - Één persoon of organisatie
  - Een beperkte groep
  - Een grote groep

7.2.2. De gegevens zijn* (?)

(?) Hebt u hulp nodig? Beschikbaarheid van de gegevens:

- *Lange periode: Gelieve dit zelf te bepalen in functie en context van de verwerkingsactiviteiten.*
- *Korte periode: Gelieve dit zelf te bepalen in functie en context van de verwerkingsactiviteiten.*

Bolean : één mogelijkheid

- Definitief onbeschikbaar
- Tijdelijk onbeschikbaar:
  - Gedurende lange periode
  - Gedurende korte periode

7.2.3. Grootte impact*

- Gegevens zijn onbetrouwbaar, onjuist en kunnen niet meer gewijzigd, gerecupereerd of hersteld worden.
- Wijzigingen aan de gegevens kunnen teruggevonden, gerecupereerd of hersteld worden o.b.v. logs en/of back-ups.

7.3. 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.

Meerdere antwoorden mogelijk

- ☐ E-mail met persoonsgegevens verstuurd naar verkeerde ontvangers (go to 7.3.1.)
- ☐ E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in cc, in plaats van bcc (go to 7.3.2.)
- ☐ Brief of pakket met persoonsgegevens werd verstuurd of afgegeven aan de verkeerde ontvanger (go to 7.3.3.)
- ☐ Autorisaties van interne of externe medewerkers verkeerd ingesteld (autorisaties ten aanzien van persoon) (?) (go to 7.3.4. en 7.3.5.)
  (?) 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) (?) (go to 7.3.6; 7.3.7 en 7.3.8.)
  (?) 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 (?) (go to 7.3.6; 7.3.7 en 7.3.8.)
  (?) 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 (go to 7.3.9; 7.3.10 en 7.3.11)
- ☐ Apparaat (mobiel, tabblad, etc.), gegevensdrager (bijv. USB-stick)en/of papier met persoonsgegevens gestolen (go to 7.3.9; 7.3.10 en 7.3.11)
- ☐ Persoonsgegevens onterecht gepubliceerd. (Bijvoorbeeld indexatie in zoekmachine; gegevens gepubliceerd op een website, op een sociaal media platform, op een papieren drager (krant, tijdschrift, etc.)) (?) (go to 7.3.12; 7.3.13. en 7.3.14.)
  (?) 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 (go to 7.3.15; 7.3.16 en 7.3.17.)
- ☐ Persoonsgegevens niet (correct) vernietigd (bijvoorbeeld leesbare persoonsgegevens bij oud papier gezet) (go to 7.3.18.)
- ☐ Persoonsgegevens onterecht vernietigd (go to 7.3.18.)

- ☐ DNS-spoofing/poisoning (?) (go to 7.3.19; 7.3.20; 7.3.21; 7.3.22)
  (?) 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 (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 en 7.3.34)
- ☐ Credential Stuffing (?) (go to 7.3.35; 7.3.36 en 7.3.37)
  (?) 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 (?) (go to 7.3.38; 7.3.39; 7.3.40 en 7.3.41.)
  (?) 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 (?) (go to 7.3.42; 7.3.43 en 7.3.44)
  (?) 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*

E-mail met persoonsgegevens verstuurd naar verkeerde ontvangers

7.3.1. Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd en de persoonsgegevens niet (verder) te gebruiken?*

Dropdown:
Ja
Nee

E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in cc, in plaats van bcc

7.3.2. Heeft u een (nieuwe) mail verstuurd naar de ontvangers in bcc waarin gevraagd wordt de voorgaande e-mail te verwijderen en de persoonsgegevens niet (verder) te gebruiken?*

Dropdown:
Ja
Nee

Brief of pakket met persoonsgegevens werd verstuurd of afgegeven aan de verkeerde ontvanger

7.3.3. Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of dat de persoonsgegevens werden teruggestuurd?

Dropdown:
Ja
Nee

Autorisaties van interne of externe medewerkers verkeerd ingesteld (autorisaties ten aanzien van persoon)

7.3.4. Heeft u de interne of externe medewerker er op gewezen dat de informatie niet verder mag worden gebruikt voor andere doeleinden?*

Dropdown:
Ja
Nee

7.3.5. Werden er kopieën genomen door de interne of externe medewerker van documenten waarin zich persoonsgegevens bevonden, waartoe deze medewerker niet geautoriseerd was?*

Dropdown:
Ja (go to 7.3.5.1.)
Nee
Niet gekend

7.3.5.1. Zijn de kopieën gerecupereerd?

Dropdown:
Ja
Nee

Netwerkmappen, applicaties of – locatie met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie (autorisaties ten aanzien van bestand) en Netwerkmappen, -applicaties of – locatie met persoonsgegevens toegankelijk van buiten de organisatie

7.3.6. Kan nagegaan worden, op basis van logbestanden of gelijkaardige instellingen, hoeveel personen toegang hebben gekregen tot de netwerkmappen, applicaties of – locaties?*

Dropdown:
Ja (go to 7.3.6.1.)
Nee

7.3.6.1. Hoeveel personen hebben onrechtmatig toegang gehad tot de netwerkmappen, applicaties of locaties*

Cijferveld

7.3.7. Kan nagegaan worden, op basis van logbestanden of gelijkaardige instellingen, wanneer personen toegang hebben gekregen tot de netwerkmappen, applicaties of – locaties?*

Dropdown:
Ja (go to 7.3.7.1.)
Nee

7.3.7.1. Wanneer vond de eerste onrechtmatige toegang plaats?*

Datumveld	*Uurveld*

7.3.8. Kan nagegaan worden of er downloads of soortgelijke kopieën werden genomen van de informatie vervat in de netwerkmappen, applicaties of -locaties?*

Dropdown:
Ja (go to 7.3.8.1.)
Nee

7.3.8.1. Zijn de downloads of soortgelijke kopieën gerecupereerd?*

Dropdown:
Ja
Nee

Apparaat (mobiel, tablet, etc.), gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens verloren en Apparaat (mobiel, tablet, etc.), gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens gestolen

7.3.9. Was het apparaat, gegevensdrager beveiligd met MFA?*

Dropdown:
Ja

Nee (go to 7.3.9.1.)

7.3.9.1. Was het apparaat, gegevensdrager beveiligd met een wachtwoord?

Dropdown:
Ja
Nee

7.3.10. Waren de persoonsgegevens op het apparaat, gegevensdrager onleesbaar gemaakt met gebruik van encryptie, hash-functies of gelijksoortige techniek?

Dropdown:
Ja (go to 7.3.10.1)
Nee

7.3.10.1. Welk concreet encryptieprotocol, hashing-functie of gelijksoortige techniek werd gebruikt?*

Meerdere antwoorden mogelijk

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Andere: *vrij tekstveld**

7.3.11. Zijn de gegevens op het apparaat in tussentijd op afstand gewist?*

Dropdown:
Ja
Nee

Persoonsgegevens onterecht gepubliceerd. (Bijvoorbeeld indexatie in zoekmachine; gegevens gepubliceerd op een website, op een sociaal media platform, op een papieren drager (krant, tijdschrift, etc.))

7.3.12. Waar (locatie) werden de persoonsgegevens precies gepubliceerd?*

Vrij tekstveld

7.3.13. Zijn de onterecht gepubliceerde persoonsgegevens nog bereikbaar?*

Dropdown:
Ja
Nee (go to 7.3.13.1.)

7.3.13.1. Hoe lang waren de onterecht gepubliceerde persoonsgegevens bereikbaar?*

Vanaf*		Tot*	
Datum	*Uur*	*Datum*	*Uur*

7.3.14. Kan nagegaan worden hoeveel personen onrechtmatig kennis hebben genomen van de onterecht gepubliceerde persoonsgegevens?*

Dropdown:
Ja (go to 7.3.14.1.)
Nee

7.3.14.1. Hoeveel personen hebben kennis genomen van de onterecht gepubliceerde persoonsgegevens?*

Aantal personen: cijfer

Persoonsgegevens van verkeerde persoon getoond in persoonlijk portaal of soortgelijke omgeving

7.3.15. Wat was de oorzaak (systeemupdate, bug, foute instelling, homoniem,…) waardoor de persoon of personen persoonsgegevens van een andere betrokkenen te zien kregen?*

Vrij tekstveld

7.3.16. Heeft u de personen er op gewezen dat men de persoonsgegevens van de andere betrokkenen niet verder mag gebruiken?*

Dropdown:
Ja
Nee

7.3.17. Werden de betrokkenen waarvan de persoonsgegevens onterecht bij de andere personen werden getoond op de hoogte gebracht?*

Dropdown:
Ja
Nee

Persoonsgegevens niet (correct) vernietigd (bijvoorbeeld leesbare persoonsgegevens bij oud papier gezet) en Persoonsgegevens onterecht vernietigd

7.3.18. Beschikt u over een beleid/procedure voor het vernietigen van persoonsgegevens?*

Dropdown:
Ja
Nee

DNS-spoofing/poisoning

7.3.19. Beschikt u over het webadres en/of IP-adres van de kloon?*

Dropdown:
Ja (go to 7.3.19.1)

Nee

7.3.19.1. Gelieve het web- of IP-adres van de kloon over te dragen

Vrij tekstveld

7.3.20. Maakt uw website gebruik van het Transport Layer Security Protocol (TLS)?*(?)

(?) Hebt u hulp nodig? Gebruik TLS-protocol: Het TLS-protocol (Transport Layer Security) is een cryptografisch protocol dat veilige communicatie over een netwerk, zoals het internet, mogelijk maakt. Het versleutelt gegevens en zorgt voor authenticatie en integriteit, waardoor informatie zoals wachtwoorden, creditcardgegevens en e-mails beschermd blijft tegen afluisteren en manipulatie.

Dropdown:
Ja
Nee

7.3.21. Beschikt uw website over een functionerend SSL-certificaat?*(?)

(?) Hebt u hulp nodig? SSL-certificaat: Een SSL-certificaat (Secure Sockets Layer) is een digitaal certificaat dat veilige communicatie tussen een website en een gebruiker mogelijk maakt. Het versleutelt gegevens, zoals wachtwoorden en creditcardinformatie, en zorgt ervoor dat de verbinding betrouwbaar is. SSL-certificaten bevestigen ook de identiteit van de website.

Dropdown:
Ja
Nee

7.3.22. Maakt uw website gebruik van Domain Name System Security Extension? (DNSSEC)*(?)

(?) Hebt u hulp nodig? DNSSEC: DNSSEC (Domain Name System Security Extensions) is een uitbreiding van het DNS-systeem die zorgt voor extra beveiliging door gegevens die via DNS worden opgehaald te verifiëren. Het voorkomt aanvallen zoals "cache poisoning" door te controleren of de ontvangen DNS-gegevens echt en niet gemanipuleerd zijn.

Dropdown:
Ja
Nee

Phishing

7.3.23. Via welk kanaal werd de phishing uitgevoerd?* (?)

(?) Hebt u hulp nodig?

- *Vishing: phishing(-pogingen) via telefoongesprekken.*
- *Smishing: phishing(-pogingen) via sms-berichten*

Dropdown:
Mailverkeer
Vishing
Smishing en phishing via andere berichtplatformen (whatsapp, telegram, signal,...)

7.3.24. Over welke soort phishing gaat het?* (?)

(?) Hebt u hulp nodig?

Spearphishing: Spearphishing valt een specifieke persoon of organisatie aan, vaak met inhoud die is toegesneden op het slachtoffer of de slachtoffers. Voorafgaand aan de aanval is meestal verkenningswerk vereist om namen, functietitels, e-mailadressen en dergelijke te ontdekken. De hackers speuren internet af om deze informatie te koppelen aan andere opgezochte kennis over de collega's van het doelwit, samen met de namen en werkrelaties van belangrijke medewerkers in diens organisatie. Hiermee construeert de phisher een geloofwaardige phishingbericht

Whaling/CEO-fraude: phishing gericht op een beslissingsnemer op hoog niveau in de organisatie. CEO-fraude (of whaling) is een vorm van cybercriminaliteit waarbij een fraudeur een e-mail stuurt vanuit een hooggeplaatste medewerker, zoals een CEO of CFO. Met als doel om mensen geld over te laten maken naar de bankrekening van de fraudeur. CEO-fraude is dus ook een vorm van betalingsfraude

Clone-phishing: een phishing-aanval waarbij de aanvaller een replica maakt van een legitieme website of e-mail om gebruikers te verleiden om hun persoonlijke gegevens in te voeren. Bij deze aanval maken criminelen een kopie — of kloon — van eerdere bezorgde en legitieme e-mails die een koppeling of een bijlage bevatten. Vervolgens vervangt de phisher de koppelingen of de bestanden in bijlage door kwaadaardige substituten die vermomd zijn als de oorspronkelijke koppelingen of bestanden.

Scareware: bijvoorbeeld: E-mailbericht waarin wordt aangestuurd dat u een pedofiel bent en dat de politie weet dat u website X hebt bezocht; E-mailbericht waarin wordt gewezen op het feit dat u een bevestiging dient te maken van uw bankrekening anders hebt u geen toegang meer tot bankrekening X; E-mail bericht waarin "dringende actie" wordt gevraagd;

Dropdown:
spearphishing
Whaling/CEO-fraude
Clonephishing
Scareware
Spoofing
Andere soort Phishing

7.3.25. Heeft de gephishte persoon zijn credentials ingegeven (gebruikersnaam, paswoord,...)?*

Dropdown:
Ja
Nee

7.3.26. Beschikte de gephishte account over MFA op het moment van de gegevensinbreuk?* (?)

(?)Hebt u hulp nodig? Multi-Factor Authentication: MFA (Multi-Factor Authentication) is een beveiligingsmethode waarbij je meerdere manieren gebruikt om je identiteit te bevestigen, zoals een wachtwoord en een code die naar je telefoon wordt gestuurd.

Dropdown:
Ja
Nee

7.3.27. Beschikte de gephishte account over een waarschuwingssysteem of gelijkaardig notificatiesysteem op het moment van de gegevensinbreuk waarbij een melding wordt gegenereerd indien een inlog(poging) vanuit een verdachte/niet-gekende locatie wordt verricht?*

Dropdown:
Ja
Nee

7.3.28. Werden er vanuit het gephishte account nieuwe phishing-mails/berichten verstuurd?*

Dropdown:
Ja (go to 7.3.28.1 en 7.3.28.2)
Nee
Niet gekend (go to 7.3.28.2)

7.3.28.1. Hoeveel phishing-mails/berichten werden verstuurd vanuit de gephishte account?*

Dropdown:
Het exacte aantal verstuurde phishing mails is gekend: *aantal*
Het extacte aantal verstuurde phishing mails is niet gekend, maar wordt geschat op: *aantal*

7.3.28.2. Heeft u een waarschuwingsbericht verstuurd naar de ontvangers van de phishing-mails/berichten vanuit de gephishte account indien u over de lijst van de ontvangers beschikt. Indien u hierover niet beschikt heeft u naar alle contactpersonen een waarschuwingsbericht gestuurd?*

Dropdown:
Ja
Nee

7.3.29. Heeft u of een externe partij een onderzoek verricht naar de oorzaak en/of omvang van de

gegevensinbreuk, zoals tot welke documenten, e-mails en andere locaties ongeoorloofde toegang kon worden verschaft met het gecompromitteerd account inclusief de daarin vervatte persoonsgegevens?*

Dropdown:
Ja
Nee
Onderzoek nog niet afgerond (go to 7.3.29.1.)

7.3.29.1. Datum waarop de resultaten van de gegevensinbreuk-onderzoek waarschijnlijk beschikbaar zullen zijn*

Datumveld

Ransomware

7.3.30. Liet de ransomware-groep/hacker een ransomware-note na?*

Drop down
Ja
Nee

7.3.31. Beschikt de organisatie over een niet-gecompromitteerde back-up na de Ransomware-aanval?*

Dropdown:
Ja
Nee
Kan niet met zekerheid worden bepaald (op dit moment)

7.3.32. Is er onrechtmatige toegang genomen tot persoonsgegevens?*

Dropdown:
Ja (go to 7.3.32.1.)
Nee
Kan niet met zekerheid worden bepaald (op dit moment) (go to 7.3.32.1.)

7.3.32.1. Waren de persoonsgegevens waartoe (mogelijks) toegang werd genomen geëncrypteerd/gehasht of anderszins onleesbaar gemaakt voor de toegang plaatsvond?*

Dropdown:
Ja (go to 7.3.32.1.1)
Nee

7.3.32.1.1. Welk concreet encryptieprotocol, hashing-functie of gelijksoortige techniek werd gebruikt?*

Meerdere antwoorden mogelijk

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Andere: *vrij tekstveld**

7.3.33. Vond er exfiltratie van persoonsgegevens plaats?*

Dropdown:
Ja (go to 7.3.33.1.)
Nee
Kan niet met zekerheid worden bepaald (op dit moment) (go to 7.3.33.1.)

7.3.33.1. Waren de persoonsgegevens die (mogelijks) werden geëxfiltreerd geëncrypteerd/gehasht of anderszins onleesbaar gemaakt voor de exfiltratie plaatsvond?*

Dropdown:
Ja (go to 7.3.33.1.1.)
Nee

7.3.33.1.1. Welk concreet encryptieprotocol, hashing-functie of gelijksoortige techniek werd gebruikt?*

Meerdere antwoorden mogelijk

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3

□ Andere: *vrij tekstveld**

7.3.34. Heeft u of een externe partij een onderzoek verricht naar de oorzaak en/of omvang van de gegevensinbreuk, zoals tot welke documenten, e-mails en andere locaties (mogelijks) ongeoorloofde toegang werd genomen en/of welke persoonsgegevens (mogelijks) geëxfiltreerd werden?

Dropdown:
Ja
Nee
Onderzoek nog niet afgerond (go to 7.3.34.1.)

7.3.34.1. Datum waarop de resultaten van de gegevensinbreuk-onderzoek waarschijnlijk beschikbaar zullen zijn*

Datumveld

Credential stuffing

7.3.35. Beschikten de accounts waartoe toegang is genomen ingevolge de credential stuffing attack over MFA?*(?)

(?)Hebt u hulp nodig? Multi-Factor Authentication: MFA (Multi-Factor Authentication) is een beveiligingsmethode waarbij je meerdere manieren gebruikt om je identiteit te bevestigen, zoals een wachtwoord en een code die naar je telefoon wordt gestuurd.

Dropdown:
Ja
Nee (go to 7.3.35.1.; 7.3.35.2; 7.3.35.3 en 7.3.35.4)

7.3.35.1. Wordt er voorzien in een CAPTCHA of gelijkaardige puzzel bij het inloggen van de accounts?*

Drop down
Ja
Nee

7.3.35.2. Doet uw organisatie aan IP-blocking, zoals geo-blocking of blacklisten van bepaalde IP adressen?*

Drop down
Ja
Nee

7.3.35.3. Voorziet uw organisatie in een maximaal aantal inlogpogingen binnen een bepaald tijdsbestek vanuit een bepaald IP-adres, ten aanzien van een account, of soortgelijke beperking?*

Drop down
Ja
Nee

7.3.35.4. Voorziet uw organisatie in andere preventiemaatregelen om credential stuffing tegen te gaan?*

Vrij tekstveld

7.3.36. Heeft u de betrokkenen van de gecompromitteerde accounts ingelicht over het feit dat er (poging) tot onrechtmatige toegang heeft plaatsgevonden tot hun accounts; en dat indien zij dezelfde credentials elders gebruiken deze mogelijks eveneens gecompromitteerd zijn?*

Drop down
Ja
Nee

7.3.37. Heeft u of een externe partij een onderzoek verricht naar de oorzaak en/of omvang van de gegevensinbreuk?*

Dropdown:
Ja
Nee
Onderzoek nog niet afgerond (go to 7.3.37.1.)

7.3.37.1. Datum waarop de resultaten van de gegevensinbreuk-onderzoek waarschijnlijk beschikbaar zullen zijn*

Datumveld

SQL-Injection

7.3.38. Maakt u gebruik van prepared statements/parametrized queries?*

Drop down
Ja
Nee

7.3.39. Was het mogelijk om van buitenaf met de applicatie te connecteren als root user?*

Drop down
Ja
Nee

7.3.40. Maakt u gebruik sanitization libraries of andere sanitiseringsmechanismen om de gegevens in de database “proper” te maken?*

Drop down
Ja
Nee

7.3.41. Heeft u of een externe partij een onderzoek verricht naar de oorzaak en/of omvang van de gegevensinbreuk?*

Dropdown:
Ja
Nee
Onderzoek nog niet afgerond (go to 7.3.41.1.)

7.3.41.1. Datum waarop de resultaten van de gegevensinbreuk-onderzoek waarschijnlijk beschikbaar zullen zijn*

Datumveld

(D)DOS-Attack

7.3.42. Bleef het gedurende DDOS-attack mogelijk om te connecteren met de geïmpacteerde server door legitieme gebruikers?*

Drop down
Ja
Nee (go to 7.3.42.1.)

7.3.42.1. Was de geïmpacteerde server langer dan 24 uur onbeschikbaar?*

Drop down			
Ja			
Nee			
Downtime start*		Downtime Stop*	
Datumveld	*Uurveld*	*Datumveld*	*Uurveld*

7.3.43. Heeft u Security Information and Event Management (SIEM)-toepassingen, Endpoint Detection and Response (EDR) en/of Extended Detection and Response (XDR)-toepassingen in plaats om gegevensverkeer te monitoren en hierop te ageren?*

Drop down
Ja (go to 7.3.43.1.)
Nee

7.3.43.1. Gelieve aan te geven over welke SIEM, EDR en/of XDR-toepassingen uw organisatie beschikt*

Vrij tekstveld

7.3.44. Heeft u of een externe partij een onderzoek verricht naar de oorzaak en/of omvang van de gegevensinbreuk?*

Dropdown:
Ja
Nee
Onderzoek nog niet afgerond (go to 7.3.44.1.)

7.3.44.1. Datum waarop de resultaten van het gegevensinbreuk-onderzoek waarschijnlijk beschikbaar zullen zijn*

Datumveld

7.4. Samenvatting van de gegevensinbreuk* (?)

(?) Hebt u hulp nodig? Samenvatting van de gegevensinbreuk: 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 tekstveld – maximum 2500 tekens

7.5. Heeft de DPO een advies verstrekt over het melden van de gegevensinbreuk, de desgevallende mededeling ten aanzien van betrokkenen en/of de te nemen maatregelen?

Dropdown:
Ja
Nee

Onderzoek nog niet afgerond (go to 7.5.1.)

7.5.1. Gelieve het advies van de DPO mee te delen*

Vrij tekstveld: maximum 500 tekens

8. Beheer

8.1. Welke specifieke (technische en organisatorische) maatregelen waren in voege om de getroffen persoonsgegevens te beschermen/dit type gegevensinbreuk te voorkomen? (?)

(?) Hebt u hulp nodig? Welke specifieke (technische en organisatorische) maatregelen waren in voege om de getroffen persoonsgegevens te beschermen/dit type gegevensinbreuk te voorkomen?

Gelieve enkel maatregelen te beschrijven die direct relevant zijn om de gegevensinbreuk te voorkomen en geen algemeen overzicht te geven van alle maatregelen.

Bijvoorbeeld: pseudonimiseren, aggregatie, hashing, audit logs, multi-factor authenticatie, data afscherming/afscheiding/ identiteits- en toelatingssysteem, wipe op afstand, encryptie, firewall, wachtwoorden, …

In voege zijnde technische maatregel*	In voege zijnde organisatorische maatregel*
Toevoegen	Toevoegen
Maatregel	*Maatregel*
+	+

8.2. Welke specifieke nieuwe/bijkomende (technische en organisatorische) maatregelen werden er genomen naar aanleiding van de gegevensinbreuk? (?)

(?)Hebt u hulp nodig? Welke specifieke nieuwe/bijkomende (technische en organisatorische) maatregelen werden er genomen naar aanleiding van de gegevensinbreuk?

Gelieve enkel maatregelen te beschrijven die werden genomen naar aanleiding van de concreet voorgevallen gegevensinbreuk en geen overzicht te geven van alle maatregelen.

Bijvoorbeeld: in kaart brengen omvang gegevensinbreuk, afsluiten van de gehele of een deel van de verwerking van persoonsgegevens, wijzigen van toegangsrechten, wijzigen van default administrators en/of gebruikers wachtwoorden, wijzigen van administrator en/of authenticatiemiddelen van de gebruikers, inroepen van technische bijstand (gelieve partij te identificeren), melden van de gegevensinbreuk aan de informatieverantwoordelijke van een gekoppelde toepassing, koppeling met andere toepassingen onderbreken/beveiligen, her- of desindexeren van de gecompromitteerde gegevens, wipen met bevestiging van toestel en bevestigingssignaal van geslaagde actie door het toestel, wijzigen van het versleutelingssysteem, melding bij de gepaste handhavingsinstanties (gelieve deze te identificeren), succesvol updaten (patchen) van de systemen,… . Geef eveneens de datum van implementatie mee.

Technische maatregelen*		Organisatorische maatregelen*	
Toevoegen		Toevoegen	
Maatregel	*Datum*	*Maatregel*	*Datum*
+	+	+	+

8.3. Welke specifieke nieuwe/bijkomende (technische en/of organisatorische) maatregelen zullen er worden genomen in de toekomst (naar aanleiding van de gegevensinbreuk)? (?)

(?) Hebt u hulp nodig? Welke specifieke nieuwe/bijkomende (technische en/of organisatorische) maatregelen zullen er worden genomen in de toekomst (naar aanleiding van de gegevensinbreuk)?

Gelieve de toekomstige maatregelen te beschrijven die zullen worden genomen naar aanleiding van de concreet voorgevallen gegevensinbreuk.

Bijvoorbeeld: uitrol MFA voor alle gebruikers, wijzigen van Active Directory-structuur, segmenteren van informaticasysteem, installeren nieuwe back-up toepassing, installeren (nieuwe) EDR/XDR-toepassing,... . Geef eveneens de verwachte datum van implementatie mee.

Technische maatregelen*		Organisatorische maatregelen*	
Toevoegen		Toevoegen	
Maatregel	*Datum*	*Maatregel*	*Datum*
+	+	+	+

9. Risico

9.1. Heeft de organisatie een (algemene) methode voor het oplijsten en beoordelen (op basis van ernst en waarschijnlijkheid) van de risico's voor de rechten en vrijheden van natuurlijke personen in geval van een inbreuk in verband met persoonsgegevens?*

Drop down
Ja (go to 9.1.1.)
Nee

9.1.1. Welke methode gebruikt u hiervoor (ENISA, eigen ontwikkelde methode, andere,...)*

Drop down
ENISA
Eigen ontwikkelde methode
Andere zoals CRAMM, OWASP, FAIR privacy, NIST Privacy Risk Assessment Matrix (PRAM)

9.2. Resultaat van de analyse ten aanzien van de risico('s) voor de rechten en vrijheden van betrokkenen*

Drop down
Waarschijnlijk hoog risico
Waarschijnlijk risico
Waarschijnlijk geen Risico

9.3. Impact/gevolgen voor de betrokkenen*

- ☐ Verlies van controle over persoonsgegevens
- ☐ Er is een verlies van vertrouwelijkheid van door het beroepsgeheim (conform art. 458 Strafwetboek) beschermde persoonsgegevens
- ☐ Schendig van fysieke integriteit
- ☐ Schending van psychische integriteit
- ☐ Schending van de intieme levenssfeer (seksuele geaardheid, naaktbeelden,…)
- ☐ Misbruik van zwakke positie (bv. minderjarigen, ouderen, mindervaliden,…)
- ☐ Materiële schade
- ☐ Immateriële schade
- ☐ Tijdelijke verhindering van toegang tot dienstverlening
- ☐ Permanente verhindering van toegang tot dienstverlening
- ☐ Discriminatie
- ☐ Identiteitsdiefstal of – fraude
- ☐ Financiële verliezen
- ☐ Ongeoorloofd teniet doen van pseudonimisering
- ☐ Reputatieschade
- ☐ Beperking van de bewegingsvrijheid (bijvoorbeeld weigeren grensovergang)
- ☐ Enig ander aanzienlijk economisch of maatschappelijk nadeel (go to 9.3.1.)
- ☐ Beperking van andere vrijheden (go to 9.3.2.)
- ☐ Beperking van andere rechten (go to 9.3.3.)
- ☐ Andere impact (go to 9.3.4.)

9.3.1. Gelieve toelichting te geven bij enig ander aanzienlijk economisch of maatschappelijk nadeel*

Vrij tekstveld

9.3.2. Gelieve toelichting te geven bij beperking van andere vrijheden*

Vrij tekstveld

9.3.3. Gelieve toelichting te geven bij beperking van andere rechten*

Vrij tekstveld

9.3.4. Gelieve toelichting te geven bij andere impact*

Vrij tekstveld

10. 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.*

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

Dropdown:
Ja (go to 10.1.1.)
Nee (go to 10.2. en 10.3.)

10.1.1. Heeft u de betrokkenen individueel ingelicht?*

Dropdown:

Ja (go to 10.1.1.1.; 10.1.1.2.; 10.1.1.3.)
Nee (go to 10.1.1.4.; 10.1.1.5. en 10.3.)

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

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

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

aantal

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

Datumveld: kalender

10.1.1.4. 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)*

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

Datumveld: kalender

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

Dropdown:
Ja (go to 10.2.1.; 10.2.2.)
Nee (go to 10.3.)
Nog niet bekend (go to 10.3.)

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

Datum veld: Kalender

10.2.2. Gaat u de betrokkenen individueel inlichten?*

Dropdown:
Ja (go to 10.2.2.1; 10.2.2.2.)
Nee (go to 10.2.2.3; 10.2.2.4. en 10.3.)

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

☐ Telefonisch ☐ Per brief ☐ Per e-mail

☐ Ander kanaal: *(vrij tekstveld)*

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

Cijfer/aantal

10.2.2.3. 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)*

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

Cijfer/aantal

10.3. Gelieve de reden aan te geven om af te zien van de (individuele) mededeling ten aanzien van de betrokkenen van wie de persoonsgegevens getroffen zijn door de gegevensinbreuk*

Meerder antwoorden mogelijk

- ☐ Omdat we van oordeel zijn dat er waarschijnlijk geen hoog risico is voor de rechten en vrijheden van natuurlijke personen
- ☐ Het zou onevenredige inspanningen vergen om iedere betrokkene op individuele basis te informeren (go to 10.3.1.)
- ☐ Er waren passende technische en organisatorische maatregelen in voege op de persoonsgegevens voordat de gegevensinbreuk plaatsvond (go to 10.3.2.)
- ☐ Er werden na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico zal voordoen (go to 10.3.3.)
- ☐ Vanwege aangereikte richtsnoeren andere relevante autoriteiten, zoals rechtshandhavingsautoriteiten (go to 10.3.4. en 10.3.5.)

10.3.1. Beschikt u over de individuele (digitale) communicatiegegevens van de betrokkenen?*

Drop down
Ja *tekst: De GBA gaat ervan uit dat wanneer u beschikt over de individuele communicatiegegevens van de betrokkenen, u deze dient te gebruiken om een individuele mededeling uit te voeren. Bijgevolg kan geen toepassing worden gemaakt van het uitzonderingsregime omtrent onevenredige inspanningen.*
Nee

10.3.2. Welke maatregelen hebt u vooraf getroffen waardoor het niet nodig is om de betrokkenen te informeren?*

Vrij tekstveld

10.3.3. Welke maatregelen hebt u genomen naar aanleiding van de gegevensinbreuk waardoor het niet nodig is om betrokkenen te informeren?*

Vrij tekstveld

10.3.4. Welke Autoriteit heeft richtsnoeren aangereikt waardoor het (momenteel) niet nodig/opportuun is om betrokkenen te informeren?*

Vrij tekstveld

10.3.5. Gelieve de inhoud van het richtsnoer samen te vatten*

Vrij tekstveld

11. 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.

12. Bijlagen

Gedateerde kopie van de mededeling aan betrokkenen

Afhankelijk van de door u aangeduide antwoorden gaat het om een individuele dan wel collectieve mededeling (zie tabblad 10). Afhankelijk van de type en aard van de gegevensinbreuk dienen mogelijks ook volgende elementen te worden opgenomen in de mededeling aan betrokkenen:

- Voor persoonsgegevens van verkeerde persoon getoond in persoonlijk portaal of soortgelijke omgeving: het feit dat de persoonsgegevens van de betrokkenen bij andere natuurlijke personen werden getoond (zie tabblad 7);
- Voor *credential stuffing*: het feit dat er (poging tot) onrechtmatige toegang heeft plaatsgevonden tot de account van de betrokkenen en deze betrokkenen waarschuwen dat, indien zij dezelfde *credentials*elders gebruiken, deze accounts mogelijks ook gecompromitteerd kunnen zijn (zie tabblad 7);
- Voor *phishing*: er dient een opsplitsing te worden gemaakt in drie groepen van betrokkenen die mogelijks een mededeling dienen te ontvangen:
    - De betrokkenen van de mailbox of soortgelijke omgeving zelf (zie tabblad 7);
    - De betrokkenen aan wie mogelijke nieuwe *phishing*-berichten werden toegestuurd (zie tabblad 7);
    - De betrokkenen van wie de persoonsgegevens zich in de mailbox of soortgelijke omgeving bevonden (zie tabblad 7).

Gedateerde kopie van de uitgevoerde risicobeoordeling

Indien u een risicobeoordeling hebt uitgevoerd van de betreffende gegevensinbreuk (zie tabblad 9).

Gedateerde kopie van het onderzoeksverslag

Indien u of een derde partij onderzoek hebt gevoerd naar de oorzaak en/of omvang van de gegevensinbreuk. Het kan gaan om alle types gegevensinbreuken (zie tabblad 8). De Gegevensbeschermingsautoriteit acht het noodzakelijk dat bij volgende types van gegevensinbreuken een onderzoek wordt gevoerd en het bijhorend verslag wordt aangeleverd: DNS-spoofing/poisoning, Phishing, Ransomware, Credential Stuffing, SQL-injection, (D)DoS-attack, AI-models, Coordinated Vulnerability Disclosure Policy (zie tabblad 7).

Gedateerde kopie van de ransomware-note

Indien het gaat om een type ransomware gegevensinbreuk en indien er een ransomware-note werd nagelaten (zie tabblad 7).

Gedateerde kopie van het phishing-bericht

Indien het gaat om een type *phishing* gegevensinbreuk en indien u nog beschikt over het initiële bericht (screenshot) waarmee de *phishing*werd uitgevoerd (zie tabblad 7).

Gedateerde kopie van de notificatie van de verdachte inlogpoging

Indien het gaat om een type *phishing* gegevensinbreuk en indien u nog beschikt over de notificatie die werd gegenereerd door het waarschuwingssysteem voor verdachte inlog(pogingen) (zie tabblad 7).

Gedateerde kopie van het beleid voor het vernietigen van persoonsgegevens

Indien u over een beleid tot het vernietigen van persoonsgegevens beschikt en het gaat om volgende types gegevensinbreuken:

- Persoonsgegevens niet (correct) vernietigd (zie tabblad 7);
- Persoonsgegevens onterecht vernietigd (zie tabblad 7).

Gedateerde kopie van de communicatie met de verkeerde ontvangers

Afhankelijk van de type gegevensinbreuk kan het gaan om volgende communicaties:

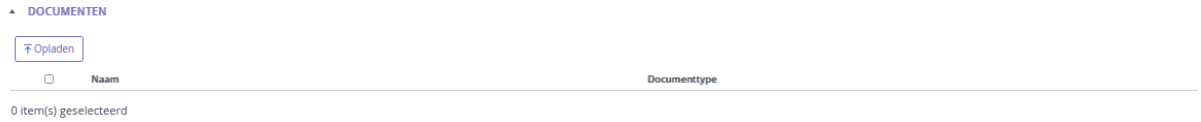
- e-mail, brief of pakket met persoonsgegevens verstuurd naar verkeerde ontvanger: communicatie waarin gevraagd wordt om de e-mail, brief of pakket te verwijderen of terug te sturen en de persoonsgegevens niet (verder) te gebruiken (zie tabblad 7);
- e-mail met persoonsgegevens verstuurd naar ontvangers in aan- of cc veld, in plaats van bcc-veld: communicatie waarin gevraagd wordt om de e-mail te verwijderen en de persoonsgegevens niet (verder) te gebruiken (zie tabblad 7);
- autorisaties ten aanzien van interne of externe medewerkers verkeerd ingesteld: communicatie aan interne of externe medewerker waarin gevraagd wordt om eventuele kopieën te verwijderen en de persoonsgegevens niet (verder) te gebruiken (zie tabblad 7);
- netwerkmappen, -applicaties of – locaties te breed ingesteld binnen of buiten de organisatie: communicatie aan interne of externe medewerker of persoon buiten de organisatie waarin gevraagd wordt om eventuele kopieën te verwijderen en om de persoonsgegevens niet (verder) te gebruiken (zie tabblad 7);
- persoonsgegevens van verkeerde persoon getoond in persoonlijk portaal of soortgelijke omgeving: communicatie aan de persoon die verkeerdelijk persoonsgegevens kon inzien van betrokkenen waarin gevraagd wordt om eventuele kopieën te verwijderen en om de persoonsgegevens niet (verder) te gebruiken (zie tabblad 7).

Gedateerde kopie van de externe melding van de gegevensinbreuk

Indien de wijze van ontdekking van de gegevensinbreuk op basis van een externe melding heeft plaatsgevonden (zie tabblad 5).

Duid aan welke bijlage u uploadt bij het indienen van de melding

- ☐ Gedateerde kopie van de mededeling aan betrokkenen
- ☐ Gedateerde kopie van de uitgevoerde risicobeoordeling
- ☐ Gedateerde kopie van het onderzoeksverslag
- ☐ Gedateerde kopie van de ransomware-note
- ☐ Gedateerde kopie van het phishing-bericht
- ☐ Gedateerde kopie van de notificatie van de verdachte inlogpoging
- ☐ Gedateerde kopie van het beleid voor het vernietigen van persoonsgegevens
- ☐ Gedateerde kopie van de communicatie met de verkeerde ontvangers
- ☐ Gedateerde kopie van externe melding van de gegevensinbreuk



13. Finaal

- ○ Ja, hierbij verklaar ik dat deel 2 volledig is
- ○ Nee, ik wens mijn wijzigingen tussentijds te bewaren en het formulier later nog aan te vullen met extra gegevens (go to 13.1 indien op bewaar wijzigingen wordt gedrukt)

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 Sorgerechtsverfügung vornehmen, werden die von Ihnen eingegebenen Werte innerhalb von 21 Tagen nach Einreichung von Teil 1 als endgültig betrachtet.