Melding van een gegevenslek, Wet van 30 juli 2018[1]

Bepaalde gegevenslekken houden de verplichting in om het Vast Comité I, gegevensbeschermingsautoriteit (DPA), op de hoogte te brengen zodra er een risico bestaat voor de fundamentele rechten en vrijheden van de betrokkenen (de personen van wie de persoonsgegevens zijn bekendgemaakt).

Dit formulier is bedoeld als basis voor deze kennisgeving.

Meldingen die niet via het formulier worden verricht, worden door het Vast Comité I niet geregistreerd als een melding van een gegevenslek maar hoogstens als een vraag of een klacht. Vermeldingen in e-mails, telefoongesprekken of alternatieve formulieren over gegevenslekken geven doorgaans onvoldoende informatie om een onderzoek toe te laten en kunnen derhalve à priori niet worden gezien als afdoende om te voldoen aan de meldingsplicht. Bovendien is er geen garantie dat deze alternatieve meldingen ook zullen worden geregistreerd en onderzocht als een melding van een gegevenslek.

De verwerkingsverantwoordelijke stelt het Vast Comité I in kennis, indien mogelijk uiterlijk 72 uur na kennisname van het gegevenslek.

Wanneer niet alle informatie beschikbaar is en de gegevenslek nader moet worden onderzocht, kan de organisatie een voorlopige melding doen. Deze voorlopige melding bevat een maximum aan antwoorden op de vragen in het formulier.

In geval van een voorlopige melding verricht de organisatie zo spoedig mogelijk een aanvullende melding. Deze aanvullende melding bevat onder meer de informatie in de andere velden van dit formulier en, eventueel, de bijgewerkte informatie ten opzichte van de voorlopige of eerste melding. Tenslotte kan ook een annulatieverzoek worden ingediend.

Het Vast Comité I vestigt uw aandacht op het feit dat dit formulier lijsten van zeer ruime categorieën van gegevens bevat, maar geenszins een impliciete toelating vormt voor de verwerking van al deze categorieën van gegevens door de verwerkingsverantwoordelijken zoals bedoeld in titel 3 van de voornoemde Wet van 30 juli 2018.

Informatie over de verwerking van persoonsgegevens

Het Vast Comité I verwerkt persoonsgegevens omdat zij daartoe wettelijk verplicht is om gegevenslekken te registeren, voor handhaving en controle en indien nodig advies te geven aan de organisatie over het gegevenslek. De persoonsgegevens worden bewaard zolang dit nodig is in het kader van adviesverlening en 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 gegevensbeschermingsautoriteiten bij gegevenslekken kunnen gegevens uit dit formulier met hen worden gedeeld.

[1] Wet van 30 juli 2018 betr. de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Deze melding betreft :	□ een volledige melding □ een annulatieverzoek van voorgaande melding □ een melding in verschillende stappen □ een aanvulling of een verbetering met betrekking tot een eerdere melding

Gelieve de onderstaande vragenlijst zo accuraat als mogelijk in te vullen. Gebruik a.u.b. duidelijk en eenvoudig taalgebruik en vermijd (waar mogelijk) terminologie die zeer technisch of juridisch is. De antwoorden kunnen steeds gestaafd worden met aanvullende documenten. In enkele gevallen worden deze documenten expliciet opgevraagd.

1. Organisatie

1.1 Hoedanigheid van de organisatie die het gegevenslek meldt

□ Verwerkingsverantwoordelijke
□ Verwerker in opdracht van een verwerkingsverantwoordelijke
□ Gezamenlijke verwerkingsverantwoordelijke

1.2 Geef de contactgegevens van de organisatie die het gegevenslek meldt

Naam van de organisatie	
Hoofdvestiging	□ in België □ in een EU of EEA land □ buiten de EU/EEA
Ondernemingsnummer [0123.456.789]	

Europees BTW-nummer	
Uniek nummer toegekend in land van registratie - verduidelijk ook welk nummer dit is	
Straat	
Huisnummer	
Bus	
Postcode	
Gemeente/Stad	
Telefoonnummer [Begin uw telefoonnummer steeds met de nationale code, voor België is dit bijvoorbeeld +32]	
Heeft de verwerkingsactiviteit betrekking op een grensoverschrijdende (internationale) verwerkingsactiviteit?	□ ja □ nee
Heeft de verwerkingsactiviteit een impact op betrokkenen in België?	□ ja □ nee
Heeft de verwerkingsactiviteit impact op betrokkenen uit een andere lidstaat of meerdere lidstaten dan België?	□ ja □ nee
Maakt deze melding onderdeel uit van een algemene kennisgeving aan andere toezichthouders op grond van andere wettelijke verplichtingen (bijvoorbeeld aan de NBB, ECB, CERT, FSMA etc.)?	
Is de verwerkingsverantwoordelijke aangemeld bij het BIPT als operator?*	□ ja □ nee
Is de verwerkingsverantwoordelijke een beursgenoteerde onderneming?	□ ja □ nee

1.3 Contactpersoon voor het gegevenslek

Hoedanigheid contactpersoon	
Naam contactpersoon	
Telefoonnummer contactpersoon [Begin uw telefoonnummer steeds met de nationale code, voor België is dit bijvoorbeeld +32]	
E-mail contactpersoon	

Is de contactpersoon een functionaris voor gegevensbescherming (hierna "DPO")? *

□ Ja;

□ Nee want de organisatie heeft geen DPO aangesteld;

□ Nee, maar de organisatie heeft een DPO, die reeds aangemeld is;

□ Nee, maar de organisatie heeft een DPO, die nog niet is aangemeld. Geef in dit geval de volledige contactgegevens van de DPO door:

2. Verwerking getroffen door het gegevenslek

Doel waarvoor de gegevens worden verwerkt	
Aard van de gegevens die getroffen zijn door het gegevenslek (Kruis één of meerdere vakjes aan)*	□ Identificatiegegevens (bijvoorbeeld naam, adres, geboortedatum, telefoonnummer, identiteitskaartnummer, rijbewijsnummer, nummerplaat, klantnummer, werknemersnummer, ...) □ Elektronische identificatiegegevens (bijvoorbeeld e-mailadressen, IP-adressen, Mac adres, sociaal netwerk, skype,...) □ Profielen (evaluatie van de betrokkene met plaatsing in een klasse of voorspelling van een bepaald kenmerk of gedrag) □ Persoonlijke kenmerken (bijvoorbeeld leeftijd, geslacht, burgerlijke staat, ...) □ CRM data (bijvoorbeeld informatie over klanten, noden, contacten, communicatie, tevredenheid etc.) □ Kopieën van paspoort, e-ID of andere legitimatiebewijzen

	□ Fysieke gegevens (bijvoorbeeld grootte, gewicht, uiterlijk,...) □ Leef-, klik-, mail-, zoek-, surf-, betaalgewoonten □ Psychische gegevens (bijvoorbeeld persoonlijkheid, karakter, ...) □ Samenstelling van het gezin □ Vrijetijdsbesteding en interesses □ Sociaal mediaprofiel □ Lidmaatschappen □ Consumptiegewoonten □ Product en dienstverlening (bijvoorbeeld bankkaartnummer, rekeningnummer, verzekeringspolisnummer, productoverzicht, salaris en inkomen, onkosten, verbruik, onderhoud, etc.) □ Woning-, autokenmerken □ Opleiding en vorming □ Beroep en betrekking, BTW-regime □ Foto's of beeldopnamen (bijvoorbeeld cctv, bewakingscamera, opgenomen opleiding etc.) □ Geluidsopnamen (bijvoorbeeld opgenomen telefoongesprekken van call center, opleiding etc.) □ HR data aangaande salaris en personeelsaanwezigheid □ HR data aangaande evaluaties, functies en opdrachten, KPI, carrièreplanning □ Fysieke beveiligingsgegevens van klanten, personeel en bezoekers (bijvoorbeeld toelatingen en rechten) □ ICT beveiligingsgegevens van klanten, personeel en bezoekers (bijvoorbeeld toelatingen en rechten, gebruik van badge, internettoegang) □ Gegevens betreffende veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (Wet van 11 december 1998) □ Gegevens m.b.t. controle op klanten □ Gegevens m.b.t. controle op personeel (bijvoorbeeld logging, klokkenluidersregeling, mandaten, preventie van handel met voorkennis, klachtenbeheer en kwaliteitscontrole, enz.) □ Gegevens m.b.t. methoden voor het verzamelen van gegevens en/of beschermings- en ondersteuningsmaatregelen (Wet van 30 november 1998) □ Nationaal nummer (bijvoorbeeld het Rijksregisternummer) □ Identificatienummer van de sociale zekerheid

	□ Raciale of etnische afkomst □ Politieke opvattingen □ Religieuze of levensbeschouwelijke overtuigingen □ Lidmaatschap van een vakbond □ Genetische gegevens (bijvoorbeeld DNA, bloedgroep,...) □ Biometrische gegevens □ Gegevens over gezondheid □ Gegevens met betrekking tot de zorg □ Gegevens over seksueel gedrag of seksuele geaardheid □ Strafrechtelijke veroordelingen □ Strafbare feiten □ Veiligheidsmaatregelen die betrekking hebben op strafrechtelijke veroordelingen of strafbare feiten □ Uittreksel uit het strafregister □ Inhoud van de elektronische communicatiegegevens □ Gegevens betreffende elektronisch communicatieverkeer □ Locatiegegevens in brede zin (bijvoorbeeld al dan niet verwerkt door telecomoperatoren of via navigatiesoftware, GPS,...) □ Financiële gegevens □ Toegangscode (wachtwoord, PIN-code, ...) □ Andere: □ Aard van de gegevens die getroffen zijn door het gegevenslek is niet gekend
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij het gegevenslek (als slachtoffer)?	Aantal personen (betrokkenen):

Van **maximaal** hoeveel personen zijn persoonsgegevens betrokken bij het gegevenslek (als slachtoffer)? Omschrijf de groep(en) van mensen van wie er persoonsgegevens zijn betrokken bij het gegevenslek.	□ Beschrijving:
Vond het gegevenslek plaats in een verwerking die is uitbesteed aan een andere organisatie?	□ Ja □ Nee

3. Beschrijving van het gegevenslek

3.1 Wat is het feit aan de oorsprong van het gegevenslek ?

De oorzaak van het gegevenslek is eerder:	□ Intern (bijvoorbeeld door personeel) □ Extern (bijvoorbeeld door een hacker)
Het gegevenslek is het resultaat van:	□ een technische werking van het systeem (niet-menselijk) □ een menselijke interventie. □ een ongeval. Specificeer: □ kwaadwillige opzet (bv. diefstal, fraude, hacken en sabotage) □ andere oorzaak

3.2 Wat is de aard van het gegevenslek ?

□ Schending van het vertrouwelijk karakter van de persoonlijke gegevens
□ Verlies van beschikbaarheid van de persoonlijke gegevens
□ Schending van de integriteit van de persoonlijke gegevens
□ Andere schending van de persoonlijke gegevens:

3.3. Geef een samenvatting van het gegevenslek

Geef bij het samenvatten van de case meer informatie over:

- het tijdstip van het gegevenslek en de ontdekking van het gegevenslek,
- genomen acties en beslissingen (tijdslijn) tot op heden,
- het technische opzet van de verwerkingsactiviteit, soort omgeving van verwerking, type van verwerking (End user computing, website beheer, operationeel beheer, big data analyse, data warehouse etc.) en de wijze van verwerken,
- de beslissing waarom het Vast Comité I werd in kennis gesteld i.p.v. andere (Belgische buitenlandse) autoriteiten.

3.4 Tijdslijn van het gegevenslek

Wanneer werd het gegevenslek ontdekt?	Datum
[UU:MM]	Tijd

Wanneer heeft het gegevenslek zich voorgedaan? [UU:MM]	□ Exacte datum en tijd waarop het gegevenslek plaatsvond is gekend, namelijk: ... □ De exacte datum en tijd van het gegevenslek is ongekend, maar wordt geschat op: ... □ Niet gekend Datum Tijd
Wanneer werden de eerste extra veiligheidsmaatregelen genomen?	□ Er werden (nog) geen extra veiligheidsmaatregelen genomen □ De eerste extra veiligheidsmaatregelen werden genomen op … en zijn:
Wanneer werd het gegevenslek verholpen?	□ Gegevenslek is nog niet verholpen. □ Gegevenslek is verholpen op … Door middel van de volgende technische of organisatorische maatregelen:
Als deze melding niet binnen de 72 uur na het ontdekken van het gegevenslek wordt verricht, wat is de reden hiervoor?	

3.5 Detectie van het gegevenslek

Wijze waarop het gegevenslek is vastgesteld*	□ Interne melding van velies van hardware of documenten □ Intern incident beheersproces (bv. ICT, incident meldingssysteem, informatieveiliheid incident management, ...) □ Interne cyber emergency team procedure □ Intern controlesysteem om indringen of lekken detecteren en ongeoorloofde toegang op te sporen □ Interne controleprocedure / klokkenluidersregeling □ Interne klachtenafhandelingsdienst □ Externe melding door een leverancier, onderaannemer of

	verwerker □ Externe melding door een klant □ Externe melding door een derde □ Externe melding door een autoriteit □ Andere, namelijk:
Welke gegevens zijn openbaar gemaakt?	□ Alle verwerkte gegevens (zie punt 2) □ Nog niet bepaald □ De volgende persoonsgegevens:

4. Preventie en beheer van gegevenslekken

Welke preventieve maatregelen waren specifiek genomen om de gelekte gegevens te beschermen? (beschrijf enkel deze maatregelen die direct relevant zijn om de inbreuk te voorkomen in plaats van een algemeen overzicht te geven van alle maatregelen) *(Bijvoorbeeld: pseudonomiseren, aggregatie, hashing, audit logs, multi-factor authenticatie, data afscherming/afscheiding/ identiteits- en toelatingssysteem, wipe op afstand, encryptie, firewall, wachtwoorden,...) Geef aan of de maatregel is ingevoerd bij het begin van de verwerking.*	Technische maatregelen: Organisatorische maatregelen:
De graad en mogelijkheid van identificatie van een betrokkene o.b.v. de onderliggende gegevens	De gegevens omvatten:

*[Zie onze handleiding voor concrete voorbeelden bij de verschillende antwoordmogelijkheden.] **	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 gelinkt 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 identiteit van de betrokkene te achterhalen.* □ Indirect tot personen 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").* Anonieme gegevens □ *Gegevens waaruit de identiteit van de betrokkenen noch direct, noch indirect blijkt, bijvoorbeeld omdat het om voldoende geaggregeerde gegevens gaat. De gegevensverzameling bevat geen individuele gegevens of minstens voldoende geaggregeerde data.*
Waren de persoonsgegevens op het moment van het ontdekken van het gegevenslek versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?	□ Ja, via welke methode : □ Nee □ Deels, namelijk:
Geplande en/of reeds ondernomen acties *(Kruis één of meerdere vakjes aan)*	□ Afsluiten van de gehele of een deel van de verwerking van persoonsgegevens □ Wijzigen van toegangsrechten □ Wijzigen van wachtwoorden administrator en/of gebruikers □ Wijzigen van administrator en/of authenticatiemiddelen van de gebruikers □ Inroepen van technische bijstand, indien zo van wie: □ Melden van het gegevenslek aan de informatieverantwoordelijke van een gekoppelde toepassing □ Koppeling met andere toepassingen onderbreken/beveiligen □ Her- of desindexeren van de gelekte gegevens (zoekmachines) □ Wipen met bevestiging van toestel en bevestigingssignaal van geslaagde actie door het toestel

	□ Wijziging van het versleutelingssysteem □ Melding bij de gepaste handhavingsinstanties, indien zo bij wie: □ Succesvol updaten (patchen) van de systemen of uitrusting □ Andere:
Zijn er relevante logs beschikbaar met betrekking tot het informatieveiligheidsincident? Zijn deze beschermd tegen ongeoorloofde wijzigingen of verwijderingen?	□ Ja, namelijk : □ Nee, de reden hiervoor is : Indien logs beschikbaar zijn, moeten deze bestanden op vraag van het Vast Comité I beschikbaar gesteld worden en gedurende het onderzoek gevrijwaard worden van wijzigingen. □ Ja, via de volgende technische middelen: □ Nee
Datum waarop de resultaten van het gegevenslekonderzoek waarschijnlijk beschikbaar zijn [UU:MM]	Datum Tijd

5. Methode voor het beoordelen van de risico's voor de rechten en vrijheden van de betrokkenen

Heeft de organisatie een algemene methode voor het oplijsten en beoordelen van de risico's voor de rechten en vrijheden van de betrokkenen in geval van een project waarbij persoonsgegevens worden verwerkt of het aanpakken van een incident met persoonsgegevens? *	□ Ja □ Nee
Worden hierbij de kans en de impact van de mogelijke nadelige	□ Ja □ Nee

gebeurtenis voor de betrokkenen nagegaan ? *	
Wat is de hoogte van de graad of het niveau van de ernst van dit gegevenslek bij het beoordelen van de risico's voor de rechten en vrijheden van de betrokkenen? *	□ Kritisch □ Hoog □ Medium □ Laag □ Verwaarloosbaar
Beschrijf beknopt de methode(s) voor het beoordelen van de risico's voor de rechten en vrijheden van de betrokkenen van een incident en de verschillende categorieën (gradaties van de risico's?) onder de gebruikte methode, of motiveer waarom u deze methode (nog) niet zou hanteren	

Welke impact kan het gegevenslek hebben voor de rechten en vrijheden van de betrokkenen (ongeacht de vraag of de kans hiertoe hoog of laag is)?

Selecteer één of meerdere opties, het risico bestaat dat

In geval van aantasting van de vertrouwelijkheid	Beschrijf het risico:
In geval van verminderde beschikbaarheid:	Beschrijf het risico:
In geval van aantasting van de integriteit:	Beschrijf het risico:
De inbreuk heeft een andere impact voor de rechten en	Beschrijf het risico:

vrijheden van de betrokkenen, namelijk kan leiden tot:	
Waarschijnlijkheid. Hoe wordt (per risico) de kans ingeschat dat voormelde impact zich voordoet ? De organisatie heeft een methode om de kans te berekenen	Beschrijf de gebruikte methode:
Gelet op de kans en impact voor de rechten en vrijheden van de betrokkenen, welke aanvullende technische en organisatorische maatregelen worden/zullen worden genomen naast de geplande acties om het (inherent) risico voor de rechten en vrijheden te beperken of te vermijden, tenzij het risico reeds voldoende werd verholpen?	Aanvullende technische maatregelen: Aanvullende organisatorische maatregelen:
Maatregelen/acties aanbevolen aan de betrokkenen *(bijvoorbeeld wijzigen van wachtwoorden)*	

6. Informatie

Hoeveel betrokken instellingen of personen heeft u geïnformeerd of gaat u informeren?	

7. Bijkomende beschouwing

Geef hier elke informatie aan die de melding beter kan doen begrijpen.	

8. Geef hier aan welke documenten u bij dit formulier toevoegt

□ Een voorbeeld van de (inhoud van de) communicatie aan de betrokkenen (indien van toepassing)

□ DPIA betreffende de verwerking (indien van toepassing)

□ Andere:

9. 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.

Data Protection Officer **Verwerkingsverantwoordelijke**