**Melding inbreuk in verband   
met persoonsgegevens**

De verwerker zal Pidpa onverwijld en gedetailleerd op de hoogte brengen en houden van iedere inbreuk die heeft plaatsgevonden bij de Verwerker. Uiterlijk binnen de 24 uur nadat de Verwerker kennis heeft genomen van een inbreuk zal hij Pidpa op de hoogte brengen en dit formulier per mail verzenden naar [IVC@pidpa.be](mailto:IVC@pidpa.be) .

Gelieve de onderstaande vragenlijst zo accuraat als mogelijk in te vullen. Indien na het invullen van dit formulier bijkomende relevante informatie beschikbaar komt, gelieve deze dan ook zo snel mogelijk via een nieuwe versie van dit formulier over te maken.

|  |
| --- |
| Datum: |
| Versie: |
| Organisatie: |
| Adres: |
| Postnummer + Gemeente/Stad: |
| Ondernemingsnummer (0123.456.789): |

|  |
| --- |
| Ik verklaar op eer dat de onderstaande inlichtingen naar waarheid worden verstrekt. |
| Naam: |
| Functie: |

|  |
| --- |
| Interne referentie naar deze melding: |

|  |
| --- |
| BESCHRIJVING VAN DE INBREUK |
| Geef een korte beschrijving van de inbreuk : |
| Beschrijving inbreuk: |

|  |
| --- |
| EVALUATIE VAN POTENTIËLE SCHADE EN RISICO |
| Hoe schat u het risico in van deze inbreuk voor de rechten en vrijheden van de betrokkenen? |
| Er bestaat geen risico |
| Er bestaat een verwaarloosbaar risico |
| Er bestaat een beperkt risico |
| Er bestaat een groot risico |
| Nog niet bepaald |
| Motivatie: |

|  |
| --- |
| CONTACTGEGEVENS |
| Wie kan gecontacteerd worden voor meer informatie over de inbreuk? |
| Naam: |
| E-mail: |
| Telefoonnummer: |

|  |
| --- |
| DETECTIE VAN DE INBREUK |
| Wanneer is de inbreuk vastgesteld? |
| Datum: |
| Uur: |
| Wie heeft de inbreuk vastgesteld? |
| Extern: Organisatie: |
| Intern: Afdeling/Functie: |
| Wijze waarop de inbreuk is vastgesteld: |

|  |
| --- |
| OORZAAK EN BESTAAN VAN DE INBREUK |
| Wanneer heeft de inbreuk plaatsgevonden? |
| Op (datum + tijd): |
| Tussen (datum + tijd) en (datum + tijd): |
| Is nog niet vastgesteld |
| Er is sprake van een anonieme melding door een derde |
| Wat is de oorzaak van de inbreuk? |
| Ongewilde ontsluiting van de gegevens |
| Hacking of malware |
| Systeemfalen |
| Toegang via ongeautoriseerde toegang |
| Toegang via geautoriseerde toegang |
| Fysiek verlies |
| Diefstal draagbaar toestel |
| Diefstal vast toestel |
| Andere: |

|  |
| --- |
| BESCHRIJVING VAN DE INBREUK EN MOGELIJKE GEVOLGEN |
| Wat is de aard van de inbreuk? |
| Aantasting van de vertrouwelijkheid: bvb. niet gemachtigde toegang / alleen lezen (Een niet-geautoriseerde Derde heeft (vertrouwelijke) data kunnen inzien. De Verwerker heeft de data nog in zijn bezit.) |
| Aantasting van de vertrouwelijkheid: bvb. verspreiding/kopiëren (Een niet-geautoriseerde Derde heeft (vertrouwelijke) data kunnen kopiëren. De Verwerker heeft de data ook nog in zijn bezit.) |
| Aantasting van de integriteit: bvb. wijziging of vervalsing van gegevens (Een niet-geautoriseerde Derde heeft (vertrouwelijke) data kunnen wijzigen in systemen van de Verwerker.) |
| Verminderde beschikbaarheid: bvb vernietiging van de gegevens (Een niet-geautoriseerde Derde heeft (vertrouwelijke) data verwijderd uit de systemen van de Verwerker of data vernietigd.) |
| Verminderde beschikbaarheid: bvb verlies of diefstal |
| Nog niet gekend |
| Wat is de aard van de gegevens die betrokken zijn bij de inbreuk? |
| Identificatiegegevens (naam, adres, telefoonnummer, …) |
| Elektronische identificatiegegevens (IP-adressen, …) |
| Elektronische lokalisatiegegevens (GSM, GPS, …) |
| Biometrische identificatiegegevens |
| Financiële gegevens |
| Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, …) |
| Fysieke gegevens (grootte, gewicht, …) |
| Leefgewoonten |
| Psychische gegevens (persoonlijkheid, karakter, …) |
| Samenstelling van het gezin |
| Vrijetijdsbesteding en interessen |
| Lidmaatschappen |
| Consumptiegewoonten |
| Woningkenmerken |
| Opleiding en vorming |
| Beroep en betrekking |
| Beeldopnamen |
| Geluidsopnamen |
| Rijksregisternummer/identificatienummer van de sociale zekerheid |
| Gevoelige gegevens (art. 6 Privacywet) |
| Raciale of etnische gegevens |
| Gegevens over het seksuele leven |
| Politieke opvattingen |
| Lidmaatschap van een vakvereniging |
| Filosofische of religieuze overtuigingen |
| Gegevens betreffende de gezondheid (art. 7 Privacywet) |
| Lichamelijke gezondheid |
| Psychische gezondheid |
| Risicosituaties en risicogedragingen |
| Genetische gegevens |
| Gegevens mbt de zorg |
| Gerechtelijke gegevens |
| Verdenkingen en inbeschuldigingstellingen |
| Veroordelingen en straffen |
| Gerechtelijke maatregelen |
| Administratieve sancties |
| DNA-gegevens |
| Andere categorieën van gegevens: |
| Wat is de omvang van de inbreuk naar aantal datarecords/documenten/mails/.... |
| Nog niet bepaald |
| Aantal betrokken datarecords/...: |
| Wat is de omvang van de inbreuk naar betrokken personen? |
| Nog niet bepaald |
| Aantal betrokken personen: |
| Omschrijf de groep personen waarvan persoonsgegevens betrokken zijn bij de inbreuk: |
| Hebben de persoonsgegevens die betrokken zijn betrekking op personen uit andere landen? |
| Nog niet bepaald |
| Nee |
| Ja, welke landen: |

|  |
| --- |
| BEHEER VAN HET INCIDENT |
| Geef een korte omschrijving van de relevante bestaande technische en organisatorische maatregelen op het moment van de inbreuk : |
| Technische maatregelen : |
| Organisatorische maatregelen : |
| Indien het om een gegevenslek gaat : |
| Het gegevenslek is afgesloten |
| Het gegevenslek is nog niet afgesloten |
| Welke acties zijn naar aanleiding van de inbreuk genomen ? |
| Afsluiten van de gehele of een deel van de dienstverlening/verwerking van persoonsgegevens |
| Wijzigen van toegangsrechten |
| Wijzigen van administrator en/of gebruikers paswoorden |
| Inroepen van technische bijstand, van wie: |
| Melden van de inbreuk aan de informatieverantwoordelijke van de betrokken dienst/verwerking |
| Koppeling met andere toepassingen onderbreken/beveiligen |
| Melding bij de gepaste autoriteit. Geef aan welke: |
| Andere: |
| Welke beveiligingsmaatregelen zijn getroffen om verdere inbreuken te voorkomen? |
| Technische maatregelen : |
| Organisatorische maatregelen : |
| Welke acties zijn gepland ? |
| Afsluiten van de gehele of een deel van de dienstverlening/verwerking van persoonsgegevens |
| Wijzigen van toegangsrechten |
| Wijzigen van administrator en/of gebruikers paswoorden |
| Inroepen van technische bijstand, van wie: |
| Melden van de inbreuk aan de informatieverantwoordelijke van de betrokken dienst/verwerking |
| Koppeling met andere toepassingen onderbreken/beveiligen |
| Melding bij de gepaste autoriteit. Geef aan welke: |
| Andere: |