**Handleiding Incidentrespons voor Inbreuken in verband met persoonsgegevens
[BEDRIJF]**

[***Opmerking: Deze sjabloon biedt een volledige stap-voor-stap checklist over hoe inbreuken in verband met persoonsgegevens tijdig moeten worden geëscaleerd. Gebruik deze sjabloon als respons op een inbreuk in verband met persoonsgegevens***]

# REIKWIJDTE

Het doel van deze Handleiding Incidentrespons voor Inbreuken in verband met persoonsgegevens (de ‘**Handleiding**’) is om u te voorzien van concrete informatie over de wijze waarop beveiligingsincidenten waarbij persoonsgegevens verloren gaan, kunnen worden geïdentificeerd en behandeld. Verlies van persoonsgegevens kan een schending vormen van wetten inzake gegevensbescherming en/of kennisgeving aan de lokale toezichthoudende autoriteiten inzake gegevensbescherming vereisen.

Alle werknemers, consultants, leveranciers en aannemers van [Bedrijf] (“[**Bedrijf**]”), op wie deze Handleiding of een deel ervan van toepassing is (“**Belanghebbenden**”) moeten deze Handleiding naleven.

De Handleiding bestaat uit de volgende belangrijke hoofdstukken:

1. **Checklist** - Een stap-voor-stap gids die de Belanghebbenden en het Responsteam inzake Inbreuken moeten volgen in het geval van een inbreuk in verband met persoonsgegevens.
2. **Schema’s** - Een reeks nuttige documenten om het Beleid en de Checklist te illustreren en aan te vullen, waaronder:
	* **Schema 1**: een sjabloonformulier om **beveiligingsincidenten te registreren** om Inbreuken in verband met persoonsgegevens binnen [Bedrijf] op systematische en consistente wijze te documenteren;
	* **Schema 2**: een beschrijving van de methodologie voor de **beoordeling van risico’s**;
	* **Schema 3**: een **sjablooncommunicatie** naar de getroffen betrokkenen of een kennisgeving aan de regelgevende instanties in verband met het ontstaan van een inbreuk in verband met persoonsgegevens.

# BELEID

* 1. **Het detecteren van en reageren op een inbreuk in verband met persoonsgegevens**

Wij hanteren een aanpak in vier stappen voor het omgaan met inbreuken in verband met persoonsgegevens, namelijk detectie, beoordeling, behandelen van respons en controle. Elk van deze stappen wordt toegelicht in paragraaf 3 (‘Checklist’).



Opsporing

Beoordeling

4. Rapportering

 en controle

Respons

Deze Handleiding doet dienst als **voorbereiding** voor alle Belanghebbenden, in afwachting van een inbreuk in verband met persoonsgegevens. Hoewel niet alle inbreuken in verband met persoonsgegevens kunnen worden vermeden, kunnen we er ons als bedrijf op voorbereiden en de impact van een inbreuk in verband met persoonsgegevens op onze organisatie aanzienlijk verminderen, zowel financieel als op het vlak van reputatie. Daarom is het belangrijk dat u zich vertrouwd maakt met deze Handleiding.

Naast de algemene voorbereiding zijn er vier andere stappen die moeten worden genomen met betrekking tot de behandeling van een inbreuk in verband met persoonsgegevens. Voor elk van deze 4 stappen hebben we een praktische checklist uitgewerkt voor de detectie, beoordeling, het antwoorden op, rapporteren over en beoordelen van een inbreuk in verband met persoonsgegevens.

* 1. **Checklist voor alle Belanghebbenden (Stap 1)**

**Stap 1 - Opsporing**

We verwachten dat inbreuken in verband met persoonsgegevens zullen worden gemeld via drie belangrijke kanalen:

* **Melding door werknemer** - Alle werknemers en andere Belanghebbenden worden aangemoedigd om een mogelijke inbreuk in verband met persoonsgegevens of bezorgdheden in dat verband te melden bij de [in te vullen door [Bedrijf]], ook al is er in die fase slechts sprake van een ernstige verdenking en geen concreet bewijs.

Wij moedigen medewerkers aan om in alle openheid feitelijke of vermoedelijke inbreuken in verband met persoonsgegevens te melden en wij zullen geen disciplinaire maatregelen nemen tegen medewerkers die mogelijk betrokken zijn geweest bij een inbreuk in verband met persoonsgegevens, op voorwaarde dat zij de inbreuk in overeenstemming met deze Handleiding melden en dat hun betrokkenheid bij de inbreuk niet opzettelijk is geweest.

* **Bewaking door** [**IT-afdeling/externe IT-dienstverlener**]- Ons/onze [IT-team/IT-dienstverlener] bewaakt onze IT- en andere besturingssystemen op regelmatige wijze om potentiële beveiligingsincidenten en inbreuken in verband met persoonsgegevens op te sporen. Hoewel de meeste kleine incidenten rechtstreeks door het/de [IT-team/IT-dienstverlener] zullen worden afgehandeld (bijvoorbeeld kleine inbreuken op het beleid voor aanvaardbaar gebruik enz.), wordt verwacht dat de ernstigere incidenten worden geëscaleerd naar [het hoofd van het/de [IT-team/IT-dienstverlener]], die op zijn/haar beurt de [Privacy Officer/Compliance Manager] moet inlichten, waar nodig.
* **Meldingen door derde partijen/externen** - Als een derde partij (bv. een vertegenwoordiger van een klant of leverancier) zich bewust wordt van een feitelijk of mogelijk veiligheidsincident of een inbreuk in verband met persoonsgegevens, is het belangrijk dat elke melding die aan ons wordt gedaan, naar behoren wordt vastgelegd en beoordeeld. Bovendien moeten derde partijen die verwerkingen doen namens [Bedrijf] contractueel verplicht worden ons van een inbreuk in verband met persoonsgegevens op de hoogte te stellen. Alle derde partijen zullen worden opgedragen om elk incident of elke inbreuk in verband met persoonsgegevens te melden aan de [Privacy Officer/Compliance Manager].

Werknemers worden geacht proactief te zijn bij het escaleren van informatie die door derde partijen over mogelijke inbreuken in verband met persoonsgegevens wordt verstrekt aan de [Privacy Officer/Compliance Manager].

Wanneer u zich bewust wordt van een incident dat naar uw mening een inbreuk in verband met persoonsgegevens inhoudt, moet u de volgende stappen volgen. Houd er rekening mee dat, afhankelijk van de concrete omstandigheden, de relevantie van de volgorde hieronder kan veranderen.

|  |
| --- |
| **STAP 1 - OPSPORING** |
| **Nr.** | **Actie** | **Eigenaar** |
| 1 | Escaleer het incident naar de [Privacy Officer/Compliance Manager]. Contactgegevens van de [Privacy Officer/Compliance Manager] zijn te vinden in [Schema 2] van deze Handleiding. | Alle Belanghebbenden |
| 2 | Wanneer het/de [IT-team/IT-dienstverlener] op de hoogte wordt gebracht van een inbreuk in verband met persoonsgegevens, zullen zij ook de [Privacy Officer/Compliance Manager] op de hoogte brengen. |
| 3 | Indien vereist of gevraagd, verleen de nodige ondersteuning aan de [Privacy Officer/Compliance Manager] naar best vermogen.  |
| 4 | Bewaar alle relevante documentatie die kan helpen bij het registreren van het incident achteraf. Zie het sjabloonformulier in Schema 1 van deze Handleiding voor meer informatie over de informatie die gewoonlijk vereist is om een incident te registreren. |
| 5 | Communiceer niet over de inbreuk aan anderen in uw team voor wie de informatie niet strikt noodzakelijk is, noch aan personen buiten [Bedrijf]. |
| 6 | Onderzoek geen computers en getroffen systemen zonder goedkeuring van IT. |
| 7 | Schakel geen computers of getroffen systemen uit zonder goedkeuring van IT. |
| 8 | Maak geen afbeeldingen of kopieën van gegevens, en sluit geen opslagapparaten/media aan op getroffen systemen. |
| 9 | Voer geen antivirusprogramma’s of -hulpprogramma’s uit zonder goedkeuring van IT. |
| 10 | Sluit geen getroffen systemen opnieuw aan zonder goedkeuring van IT. |

**Stap 2 - Beoordeling**

Na detectie van een (potentiële) inbreuk in verband met persoonsgegevens zal de [Privacy Officer/Compliance Manager] - na op de hoogte te zijn gebracht door een werknemer, het/de [IT-team/IT-dienstverlener] of een derde partij - de verdere procedure leiden inzake incidentrespons. Voor deze fase moeten de volgende stappen worden gevolgd, al dan niet in chronologische volgorde, afhankelijk van de concrete omstandigheden:

|  |
| --- |
| **STAP 2 - BEOORDELING**  |
| **Nr.** | **Actie** | **Eigenaar** |
| 1 | Draag het/de [IT-team/IT-dienstverlener]/Hoofd van het/de [IT-team/IT-dienstverlener] op om de eerste technische beoordeling van de mogelijke inbreuk in verband met persoonsgegevens te beheren. | [Privacy Officer/Compliance Manager] |
| 2 | Draag het/de [IT-team/IT-dienstverlener] op om in geval van een inbreuk een technische beoordeling van de ernst van de inbreuk uit te voeren, met inbegrip van de aard van de geraadpleegde informatie en de omvang van de toegang.  | [Hoofd van het IT-team/IT-dienstverlener] |
| 3 | Ken de relevante toegangsmachtigingen toe aan leden van het/de [IT-team/IT-dienstverlener] waar nodig. | [Hoofd van het IT-team/IT-dienstverlener] |
| 4 | Communiceer bevindingen van de technische beoordeling aan de [Privacy Officer/Compliance Manager]. | [Hoofd van het IT-team/IT-dienstverlener] |
| 5 | Vraag bijkomend onderzoek aan over de inbreuk in verband met persoonsgegevens bij het/de [IT-team/IT-dienstverlener] waar nodig. | [Privacy Officer/Compliance Manager] |

**Stap 3 - Respons**

Zodra de eerste technische beoordeling van de inbreuk in verband met persoonsgegevens is uitgevoerd, moet het incident worden aangepakt op een wijze die is afgestemd op de kenmerken ervan en de omstandigheden rond het incident.

Op basis van de bevindingen van de technische beoordeling, moet het [in te vullen door [Bedrijf]] de respons coördineren en op regelmatige tijdstippen rapporteren aan de [in te vullen door [Bedrijf]], zoals met deze laatste overeengekomen.

Als op basis van de aard van de inbreuk blijkt dat e-mailsystemen van [Bedrijf] gecompromitteerd kunnen zijn, moet worden overwogen om telefonisch te communiceren om te voorkomen dat essentiële communicatie lekt.

| **STAP 3 - RESPONS**  |
| --- |
| **Nr.** | **Algemene actie** | **Specifieke actiestappen** | **Eigenaar** |
| 1 | **Interne beoordeling** - Richt een responsteam inzake inbreuken op en organiseer een vergadering waar u beraadslaagt en de tot dan toe bekende feiten bespreekt, inclusief de aard van de geraadpleegde informatie en de omvang van de toegang.Dit omvat doorgaans details over wie betrokken was, wat er is gebeurd, waar het is gebeurd, wanneer het is gebeurd, hoe het is gebeurd en hoe [Bedrijf] de inbreuk kan verhelpen.De besprekingen moeten gebaseerd zijn op de eerste technische beoordeling die wordt verzorgd door het [Hoofd van het/de [IT-team/IT-dienstverlener]]. | 1. Neem contact op met een externe adviseur om de juridische gevolgen van de inbreuk te begrijpen en een juridische strategie te bevestigen.
2. Richt een vertrouwelijke portaalsite op voor het responsteam inzake inbreuken om de acties te registreren die zijn ondernomen om juridisch advies en juridische leiding te geven.
3. Ontwerp van een (voorlopig schema van een) strategie voor de respons op inbreuken, inclusief de te nemen acties en de eigenaar van elke actie.
 | a) [Hoofd van het/de [IT-team/IT-dienstverlener]]b) [Privacy Officer/Compliance Manager] c) andere Belanghebbenden afhankelijk van de omstandigheden van de inbreuk in verband met persoonsgegevens |
| 2 | **Onderzoek** - Het team moet beoordelen of de informatie en bevindingen die tot nu toe zijn verzameld met betrekking tot de inbreuk, voldoende zijn om de aard van het incident en de gevolgen voor de organisatie (op het vlak van wettelijke aansprakelijkheid, reputatieschade, financiële gevolgen, organisatorische gevolgen en andere risicofactoren) te begrijpen, en voldoende helpen om de onderliggende oorzaak en de getroffen belanghebbenden vast te stellen. | 1. Informeer het team over inperking, de status van het onderzoek en andere relevante aspecten.
2. Beoordeel de volledigheid en juistheid van de tot dan toe verzamelde informatie.
3. Waar nodig: aanvullend onderzoek laten uitvoeren door personeel van het/de [IT-team/IT-dienstverlener], externe cyberbeveiliging en/of forensische deskundigen.
4. Bepalen hoe de inbreuk moet worden aangepakt terwijl de bedrijfscontinuïteit wordt verzekerd of hersteld.
5. Identificeer de personen die waren betrokken bij de ontdekking en het eerste onderzoek van de inbreuk. Documenteer hun acties en bevindingen, organiseer interviews met deze personen waar nodig om ontbrekende informatie te bekomen.
6. Overweeg om rekening houdend met de stand van het onderzoek, het Uitvoerend Comité en de Raad van Bestuur, naargelang het geval, in te lichten [OPTIONEEL].
 | a) [Hoofd van het/de [IT-team/IT-dienstverlener]][Door externe deskundigen te behouden, kan de communicatie die voor of door de externe deskundigen is voorbereid, worden beschermd door het verschoningsrecht (attorney-client privilege).]b) [Privacy Officer/Compliance Manager] c) andere Belanghebbenden afhankelijk van de omstandigheden van de inbreuk in verband met persoonsgegevens |
| 3 | **Inperking** - Bespreek welke stappen moeten worden ondernomen om de inbreuk in te perken, teneinde verder gegevensverlies of aantasting van de beveiliging te voorkomen.  | 1. Als de inbreuk nog bezig is, raadpleeg dan forensische deskundigen [en opgeleid [Informatiebeveiligings] personeel] over het offline halen van de getroffen systemen door ze los te koppelen van het netwerk, en/of gebruik te maken van tools om van de getroffen systemen dynamisch een image te maken om bewijsmateriaal te bewaren.
2. Indien de inbreuk geen betrekking heeft op persoonsgegevens van werknemers, overweeg dan werknemers op de hoogte te brengen van de inbreuk om ervoor te zorgen dat passende maatregelen worden genomen om de inbreuk op individueel niveau in te perken.
3. Wijzig waar nodig apparaten inzake beveiliging van toegang en wachtwoorden.
4. Als de inbreuk een inbreuk op betaalkaartgegevens inhoudt, vraag dan juridische hulp over de aanvullende stappen die moeten worden genomen en vraag zo snel mogelijk een lijst van de getroffen creditcardnummers op.
5. Bepaal eventuele juridische gevolgen van vrijwaring en/of aansprakelijkheid van derde partijen indien de inbreuk is veroorzaakt door een derde.
 | a) [Hoofd van het/de [IT-team/IT-dienstverlener]][Door externe deskundigen te behouden via de Juridische afdeling, kan de communicatie die voor of door de externe deskundigen is voorbereid, worden beschermd door het verschoningsrecht (attorney-client privilege).]b) [Privacy Officer/Compliance Manager] c) andere Belanghebbenden afhankelijk van de omstandigheden van de inbreuk in verband met persoonsgegevens |
| 4 | **Herstel** - Herstel van de diensten die door de inbreuk zijn getroffen, zo snel mogelijk nadat de inbreuk is ingeperkt. | Dit kan het herstellen van gegevens van geschikte back-upsystemen omvatten, mits alle sporen van de inbreuk zijn verwijderd. | [Hoofd van het/de [IT-team/IT-dienstverlener]] |
| 5 | **Interventie en verbetering** - Interventie- en verbeterprocessen toepassen op bestaande bedrijfsprocessen om herhaling van het incident te voorkomen.  | Dit kan worden ondersteund door gerichte bewustmakingstraining inzake beveiliging of juridische stappen. | [in te vullen door [Bedrijf]] |
| 6 | **Bewaring van bewijsmateriaal** - Als wordt besloten om een dader van de inbreuk in verband met persoonsgegevens te vervolgen, is het essentieel om een forensische kopie van het getroffen systeem te nemen onmiddellijk nadat de inbreuk op de beveiliging werd ontdekt als bewijs van de inbreuk. | 1. Raadpleeg deskundigen op het gebied van cyberbeveiliging en forensisch onderzoek voordat gegevens worden ‘aangeraakt’ die mogelijk betrokken zijn bij het incident.
2. Bewaar alle getroffen systeemlogbestanden, inclusief de logbestanden van firewalls, VPN’s, e-mails, netwerken, cliënten, websites, servers en inbraakdetectiesystemen.
 | a) [Hoofd van het/de [IT-team/IT-dienstverlener]]b) [Privacy Officer/Compliance Manager]  |
| 7 | **Documentatie -** Bewaar geschikte documentatie over de inbreuk in verband met persoonsgegevens. Systeemlogbestanden zijn van cruciaal belang voor het beoordelen van de oorsprong van de aanval, de duur ervan en de hoeveelheid gegevens die tijdens de inbreuk werden getroffen. Deze informatie kan bijdragen tot het opstellen van een ‘lessons learned’. | 1. Registreer de datum en het tijdstip van de inbreuk, het personeel dat de inbreuk heeft ontdekt, de aard van de inbreuk, de soorten gestolen/verloren gegevens, het tijdstip van de respons en alle werknemers die toegang hadden tot de getroffen systemen. Cf. Schema 1 voor een sjabloonformulier voor een logbestand.
2. Bevestiging dat de beveiligingstoegang is beëindigd voor elke werknemer die ervan wordt verdacht opzettelijk bij de inbreuk betrokken te zijn geweest.
 | a) [Hoofd van het/de [IT-team/IT-dienstverlener]] |
| 8 | **Betrokkenheid van belanghebbenden (melding)** - Het is belangrijk om degenen die rechtstreeks door de inbreuk worden getroffen of die een groter belang kunnen hebben bij het beheer van de inbreuk op doeltreffende wijze te betrekken. Waarschijnlijk gaat het daarbij om werknemers, de media, klanten en toepasselijke regelgevende instanties of wetshandhavingsinstanties. Een plan inzake betrokkenheid moet zo snel mogelijk worden afgesproken.Merk op dat afhankelijk van de specifieke omstandigheden en het juridische advies dat wordt ingewonnen bij een plaatselijke externe raadsman, **het wettelijk verplicht kan zijn om de getroffen personen, wetshandhavingsinstanties en/of regelgevende instanties in een vroeger stadium op de hoogte te brengen en meer specifiek binnen 72 uur in geval van inbreuken in verband met persoonsgegevens die Europese entiteiten treffen.**Zie de onderstaande tabel voor meer informatie. | 1. Raadpleeg de onderstaande tabel voor specifieke acties inzake meldingen met betrekking tot elke categorie van betrokken persoon of autoriteit.
2. Bepaal wie verantwoordelijk is voor de melding ([Bedrijf], of een klant of leverancier).
3. Ontwikkel een plan inzake betrokkenheid/communicatie.
 | a) [Hoofd van de getroffen afdelingen]b) [Privacy Officer/Compliance Manager] c) andere Belanghebbenden afhankelijk van de omstandigheden van de inbreuk in verband met persoonsgegevens (bv. in dit geval de Juridische afdeling, Personeelsafdeling.) |
| 9 | Blijf indien nodig teamvergaderingen bijeenroepen. | Blijf de strategie voor de respons op inbreuken bijsturen en de voortgang op de actielijst opvolgen. | Responsteam inzake inbreuken |
| 10 | Blijf het Uitvoerend Comité en de Raad van Bestuur, naargelang het geval, verder inlichten. | N.V.T. | [Privacy Officer/Compliance Manager]  |

**Melding aan en betrokkenheid van belanghebbenden**

Met betrekking tot de melding moet advies worden ingewonnen bij de [juridische afdeling/externe juridische adviseur] voordat u contact opneemt met het personeel of externe belanghebbenden om ervoor te zorgen dat de verstrekte informatie juist is en ons niet blootstelt aan onnodige risico’s. De [juridische afdeling/externe juridische adviseur] zal bepalen of en hoe inbreuken in verband met persoonsgegevens moeten worden gemeld, aangezien de meldingsplicht van land tot land kan verschillen en ongepaste acties tot rechtshandhavingsmaatregelen kunnen leiden.

De onderstaande tabel biedt een overzicht van de goede praktijken inzake de melding aan belanghebbenden. De melding aan of de betrokkenheid van deze belanghebbenden mag uitsluitend plaatsvinden in strikte overeenstemming met het door het responsteam inzake inbreuken ontwikkelde plan inzake betrokkenheid, en alleen door personen die uitdrukkelijk voor een dergelijke betrokkenheid gemachtigd zijn. Met uitzondering van het personeel, moeten we zorgvuldig evalueren wanneer we de getroffen personen, andere derden en autoriteiten op de hoogte moeten stellen of met hen moeten communiceren wanneer dit niet wettelijk of contractueel vereist is.

| **MELDING - BETROKKENHEID VAN BELANGHEBBENDEN** |
| --- |
| **Belanghebbende** | **Actie** |
| Personeel  | * Personeel tijdig op de hoogte brengen van de juiste informatie om geruchten te beperken.
* Als er een hoog risico is voor de rechten en vrijheden van het personeel, kan het zijn dat u verplicht bent om de inbreuk in verband met persoonsgegevens onverwijld aan het personeel te melden.
* Verstuur communicatie van een vertrouwde bron met indicaties over de timing van updates.
* Voorzie instructies in alle incident-gerelateerde communicatie om ‘niet door te sturen’.
 |
| Klanten, B2B-klanten of andere betrokkenen | * Als er een hoog risico is voor de rechten en vrijheden van deze betrokkenen, kan het zijn dat u verplicht bent om de inbreuk in verband met persoonsgegevens (aan de hand van duidelijke en gedetailleerde meldingsbrieven) onverwijld aan deze betrokkenen te melden.
* Geef contactgegevens op voor klanten en/of gebruikers om aanvullende informatie te bekomen.
* Verstrek informatie over het soort gegevens dat mogelijk is blootgesteld, de mogelijke gevolgen voor klanten en/of gebruikers en de reactie van [Bedrijf].
* [OPTIONEEL] Werk samen met [Public Relations en Juridische] teams om meldingsbrieven op te stellen in overeenstemming met toepasselijke wet- en regelgeving.
 |
| [OPTIONEEL] Media | * Werk samen met de afdeling [Public Relations] om interacties met de media te behandelen en voor het ontwikkelen van een strategie voor tijdige incidentcommunicatie.
* Bereid een vooraf goedgekeurde proactieve verklaring voor die waar nodig wordt vrijgegeven met duidelijke ‘te volgen lijnen’.
* Maak een specifieke inbox voor e-mail om de communicatie met de media mogelijk te maken.
* Neem relevante juridische, ethische en reputatieschade in beschouwing bij het opstellen van persberichten.
 |
| Autoriteiten en regelgevende instanties | * Duidelijk weten wanneer er een wettelijke verplichting bestaat om een inbreuk te melden aan een regelgevende instantie (bv. toezichthoudende autoriteiten voor gegevensbescherming) of wetshandhavingsinstantie.
* Als er een hoog risico is voor de rechten en vrijheden van een betrokkene, kan het zijn dat u verplicht bent om deze betrokkene(n) op de hoogte te stellen.
* Overweeg om een regelgevende instantie of wetshandhavingsinstantie vrijwillig bij een inbreuk te betrekken (bijvoorbeeld als u vermoedt dat de inbreuk vals is), aangezien zij op basis van hun ervaring met soortgelijke incidenten kunnen helpen bij het vaststellen van de volgende stappen om de inbreuk te beheersen.
 |

**Stap 4 - Rapportering en Beoordeling**

|  |
| --- |
| **STAP 4 - RAPPORTERING EN BEOORDELING**  |
| **Nr.** | **Algemene actie** | **Specifieke actiestappen** | **Eigenaar** |
| 1 | Blijven toezien op de naleving van wettelijke verplichtingen. | Bv. verzekeren dat alle noodzakelijke meldingen over inbreuken werden gemaakt. | [in te vullen door [Bedrijf]] |
| 2 | Bewaken van de interne respons op de inbreuk en beoordelen of verdere communicatie naar werknemers nodig is. | Indien nodig, ontwikkelen en versturen van bijkomende communicatie naar de werknemers. | [Privacy Officer/Compliance Manager / HR] |
| 3 | Bewaken van de externe respons op de inbreuk en beoordelen of verdere externe communicatie naar het publiek en/of media nodig is. | 1. Indien nodig, ontwikkelen en versturen van bijkomende communicatie naar het publiek en/of de media.
2. Beoordelen of personen die door de inbreuk zijn getroffen, bijkomende informatie nodig hebben. Indien nodig, ontwikkelen en versturen van bijkomende communicatie naar de getroffen personen.
 | [Privacy Officer/Compliance Manager] |
| 4 | Afronden van het lopend onderzoek zodra het incident is opgelost. | N.V.T. | Responsteam inzake inbreuken |
| 5 | Op basis van het (de) logformulier(en) van de inbreuk een Incidentenrapport opstellen [OPTIONEEL: voor het Uitvoerend Comité en de Raad van Bestuur van [Bedrijf], indien vereist]. | Het Incidentenrapport moet het volgende bevatten:* Een samenvatting van de inbreuk (datum, omschrijving, afdeling(en) en betrokken medewerkers);
* Omvang van mogelijk getroffen regio’s/landen;
* Wie werd geïnformeerd;
* Ondernomen acties met data en eigenaren van de acties;
* Schatting van de financiële kosten en de zakelijke impact van het incident;
* Aanbevelingen voor wijzigingen om toekomstige voorvallen te voorkomen;
* Raming van het tijdschema voor de implementatie van aanbevolen wijzigingen in afwachting van goedkeuring door het management.
 | Responsteam inzake inbreuken(Externe adviseur)(Externe experten) |
| 6 | Breng alle betrokken partijen en belanghebbenden op de hoogte dat het incident is opgelost. | 1. Bereid de communicatie voor.
2. Coördineer de melding.
 | Responsteam inzake inbreuken |
| 7 | Organiseer een vergadering met het responsteam inzake inbreuken na de inbreuk. | Tijdens de vergadering moeten de volgende onderwerpen aan de orde komen:* Hebben de procedures inzake detectie en respons gewerkt zoals bedoeld?
* Indien niet, op welke gebieden is er verbetering nodig?
* Welke wijzigingen kunnen er worden aangebracht in de procedures om ons beter in staat te stellen soortgelijke incidenten op te sporen en aan te pakken?
* Welke tools werkten goed en welke extra tools zouden in de toekomst nuttig kunnen zijn?
* Was het niveau van de respons passend?
* Kunnen er lessen worden getrokken uit het incident?
 | Responsteam inzake inbreuken |
| 8 | Voeg output van de vergadering ten behoeve van de post-incidentevaluatie toe aan het Incidentenrapport. | N.V.T. | Responsteam inzake inbreuken |
| 9 | Beoordeel de operationele controles en wijzig deze waar nodig. | Dit kan een herziening omvatten van de controles op het verzamelen van gegevens, opleiding enz. | [Hoofd van het/de [IT-team/IT-dienstverlener]] |
| 10 | Beoordeel de opleidingen van het personeel, inclusief [IT-team/IT-dienstverlener], en wijzig deze waar nodig. | Herinner de betrokken partijen eraan dat potentiële bezorgdheden over incidenten moeten worden gemeld aan de [Privacy Officer/Compliance Manager]. | [Privacy Officer/Compliance Manager]/HR |

* 1. **Beoordeling en updates**

Alle updates in verband met toepasselijke voorschriften, interne operationele procedures of andere vereisten zullen onmiddellijk worden uitgevoerd door de [Privacy Officer/Compliance Manager], die alle updates aan deze Handleiding binnen een redelijke termijn zal beoordelen en deze zal laten goedkeuren door het responsteam inzake inbreuken.

Voor vragen over deze Handleiding, neem contact op met [Privacy Officer/Compliance Manager] op [voeg contactgegevens in].

##### Schema 1 - FORMULIER VOOR HET LOGGEN VAN EEN INBREUK IN VERBAND MET PERSOONSGEGEVENS

| **(Potentieel) Incidentlogboek** |
| --- |
| **Informatie** | **Omschrijving** |
| Unieke identificatie | *[Voeg naam in/conventie voor logcodes om inbreuken in verband met persoonsgegevens van elkaar te onderscheiden]* |
| Eigenaar van het incident | *[Lijst van huidige en vroegere eigenaars van de inbreuk in verband met persoonsgegevens, inclusief contactgegevens voor natuurlijke personen]* |
| Beschrijving van het incident | *[Voeg overzicht van de inbreuk in verband met persoonsgegevens in, inclusief doorzoekbare trefwoorden en vermeld getroffen gebruikers en systemen]* |
| Samenvatting van actiestappen | *[Voeg een beschrijving toe van de stappen die zijn genomen om de inbreuk in verband met persoonsgegevens in te perken en ervan te herstellen]* |
| Data en tijdstippen voor alle gebeurtenissen | *[Stel een lijst/details op van de tijdstippen van het voorvallen, ontdekken, inperken en herstellen]* |
| Identificatie van het incident | *[Nadere bijzonderheden over de identificatiemethode van de inbreuk in verband met persoonsgegevens]* |
| Niveau van ernst | *[Detail van de gevolgen van de inbreuk in verband met persoonsgegevens]* |
| Vereiste inspanningen van het personeel om het incident op te lossen | *[Stel een berekening op van de personeelsuren die nodig zijn om de inbreuk in verband met persoonsgegevens in te perken/te herstellen/op te lossen]* |
| Systeemonderbreking | *[Vermeld, indien van toepassing, het aantal uur dat een systeem niet beschikbaar was voor het bedrijf]* |
| Oplossing | *[Beschrijf hoe de inbreuk in verband met persoonsgegevens werd opgelost]* |
| Vermijdbaar incident | *[JA/NEE]* |
| Andere relevante informatie | *[Vermeld alle andere informatie die u met betrekking tot de inbreuk in verband met persoonsgegevens relevant acht.]* |

##### Schema 2 - Beoordeling van het risico

Wanneer er geen nadelige gevolgen voor personen te verwachten zijn, is er geen melding aan de betrokkenen en de toezichthoudende autoriteit nodig. Deze evaluatie is dus belangrijk en moet worden gedocumenteerd. Om deze nadelige effecten te beoordelen en de inbreuk in verband met persoonsgegevens als hoog of kritiek te categoriseren, moet met alle passende elementen rekening worden gehouden.

Merk op dat de volgende criteria **alleen dienen als leidraad** en moeten worden gewijzigd in overeenstemming met de specifieke bepalingen van [uw bedrijf]. Bovendien moeten de criteria samen worden beoordeeld en heeft het ene criterium geen prioriteit boven het andere.

1. Aantal getroffen betrokkenen

In principe is het aantal betroffen betrokkenen **geen bepalende factor** en de melding dient afhankelijk te zijn van de mogelijke negatieve gevolgen, onafhankelijk van het aantal betroffen betrokkenen.

Maar als de contactgegevens van één persoon per ongeluk worden bekendgemaakt door het sturen van een e-mail naar een derde partij, is het schijnbaar niet de moeite waard om het volledige interne en externe administratieve proces uit te voeren. Als de contactgegevens van alle werknemers van een multinational of de gegevens van alle consumenten openbaar zouden worden gemaakt, wordt voorgesteld dit te melden.

Er bestaat geen maatstaf voor deze materie en het wordt aanbevolen om in geval van twijfel een melding te doen.

1. Het type persoonsgegevens

Het type persoonsgegevens is een **essentiële en doorslaggevende** factor in de beoordeling. De gevoeligheid van de persoonsgegevens kan vereisen om een inbreuk in verband met persoonsgegevens met betrekking tot één persoon te melden.

Over het algemeen zou voor gevoelige persoonsgegevens een melding vereist zijn (iemands godsdienst of overtuiging, ras, politieke overtuiging, gezondheid, seksleven, lidmaatschap van een vakbond, alsook strafrechtelijke persoonsgegevens).

Het omvat ook gegevens die stigmatisering of uitsluiting van de betrokkene mogelijk maken, schade berokkenen aan de gezondheid, financiële schade of (identiteits) fraude kunnen veroorzaken, of gegevens die verband houden met de financiële of economische situatie van de betrokkene. Het kan ook gebruikersnamen, wachtwoorden en andere inloggegevens bevatten.

1. De op de persoonsgegevens toegepaste technologische beschermings- en organisatorische maatregelen

De toegepaste technologische beschermings- en organisatorische maatregelen zijn een andere **essentiële en doorslaggevende** factor in de beoordeling. Aangezien een melding aan de betrokkenen of een mededeling aan de toezichthoudende autoriteit vereist is wanneer de inbreuk geen negatieve gevolgen heeft voor de persoonsgegevens of de privacy van de betrokkenen. Afhankelijk van de toegepaste maatregelen kunnen er geen risico’s voor de betrokkenen aan verbonden zijn.

Hoewel deze maatregelen moeten worden **beoordeeld per geval om te bepalen of zij het risico voor de betrokkene hebben beperkt**, tonen richtlijnen van de WP29 aan de hand van voorbeelden aan wat deze maatregelen kunnen zijn.

1. De kans op grote financiële risico’s of wettelijke aansprakelijkheid voor de onderneming

Hoewel vanuit het oogpunt van de overheid de betrokkene centraal dient te staan in deze beoordeling, is het vanuit het oogpunt van uw organisatie essentieel om ook rekening te houden met de financiële risico’s en wettelijke aansprakelijkheid die u kunt lopen. Wij raden u aan om ten aanzien van uw meldings- en communicatieplicht de allerhoogste norm toe te passen wanneer u een grote financiële of juridische aansprakelijkheid riskeert waarbij rekening wordt gehouden met de impact op public relations.

##### Schema 3 - SJABLOON COMMUNICATIE/meldingen

1. **Communicatie naar werknemers of andere betrokkenen**

Afhankelijk van de omstandigheden, moet deze brief **zijn afgestemd op de feitelijke verschillen en juridische verschillen** Een inbreuk die van invloed is op werknemersgegevens of gegevens van andere betrokkenen (bv. consumenten, identificeerbare natuurlijke personen van derde partijen) vereist slechts een melding die afhankelijk is van het hoge risico voor de rechten en vrijheden van de betrokkene en de voorwaarden die [Bedrijf] heeft ingevoerd om de getroffen persoonsgegevens te beveiligen. [PERSOON INVOEGEN] zal de noodzaak evalueren om de betrokkene te informeren [en de [PERSOON INVOEGEN] op de hoogte brengen om de onderstaande verklaring aan te passen aan de omstandigheden zoals beschreven door [PERSOON OPNIEUW INVOEGEN] aan [PERSOON INVOEGEN]].

**Verklaring inzake Inbreuk in verband met persoonsgegevens**

Geachte \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Als een gewaardeerde werknemer/consument/andere betrokkene van [Bedrijf] International (‘[Bedrijf]’), schrijven we om u te informeren over een veiligheidsincident dat een invloed heeft gehad op uw persoonsgegevens. Wij nemen de veiligheid van uw persoonsgegevens ernstig en betreuren oprecht de impact die dit incident mogelijk op u heeft gehad. Lees deze brief voor meer informatie over het incident, de diensten die wij u bieden als respons erop en de stappen die u kunt ondernemen.

**Wat is er gebeurd?**

Op [DATUM] was [Bedrijf] het slachtoffer van [SPECIFIEER DE OORZAAK - bv. een phishingincident via e-mail - waarbij een van onze werknemers te goeder trouw gevoelige informatie deelde met een externe partij die zich voordeed als directielid van [Bedrijf]] hetgeen resulteerde in [SPECIFIEER HET RESULTAAT - bv. een ongeoorloofde bekendmaking van uw persoonsgegevens aan derde partijen].

**Om welke Persoonsgegevens ging het?**

De persoonsgegevens in dit incident waren onder meer [VOEG BEKENDGEMAAKTE PERSOONSGEGEVENS IN - bv. uw naam, adres, rijksregisternummer, inkomen, en ...]. Op dit moment hebben we geen reden om aan te nemen dat het om nog andere persoonsgegevens zou gaan.

**Wat zijn de mogelijke gevolgen?**

Wegens de [HERHAAL DE GEVOLGEN], worden uw persoonsgegevens in dit incident mogelijk ook bekendgemaakt aan [SPECIFIEER MOGELIJKE GEVOLGEN].

**Wat zijn we aan het doen?**

We hebben kennis genomen van het incident op [DATUM] en prompt onze procedure inzake Incidentrespons voor Inbreuken in verband met persoonsgegevens geïnitieerd met een onderzoek naar wat er is gebeurd, [externe forensische experts aangesteld] en een melding gedaan aan [VOEG WETSHANDHAVINGS- EN/OF KREDIETBUREAUS IN].

Bovendien doen we [VOEG ANDERE STAPPEN IN DIE [Bedrijf] AAN HET NEMEN IS ALS RESPONS OP HET INCIDENT].

Wij nemen de veiligheid van uw persoonsgegevens ernstig en bieden aan iedereen die mogelijk hinder heeft ondervonden onze oprechte excuses aan. Om u te helpen bij de bescherming van uw persoonsgegevens tegen [VOEG MOGELIJK RESULTAAT IN], bieden wij de volgende diensten aan:

* [VOEG MOGELIJKE DIENST IN OM HET RESULTAAT TE REMEDIËREN]. Deze [...] helpt om [VOEG IN WAT DE DIENST ZAL DOEN - bv. het detecteren van mogelijk misbruik van uw persoonsgegevens en biedt u ondersteuning bij identiteitsbescherming gericht op de onmiddellijke identificatie en oplossing van potentiële identiteitsdiefstal en HOE zij de dienst kunnen aanvragen.]
* [VOEG MOGELIJKE DIENST IN OM HET RESULTAAT TE REMEDIËREN]. Deze [...] helpt om [VOEG IN WAT DE DIENST ZAL DOEN en HOE zij de dienst kunnen aanvragen]
* [VOEG MOGELIJKE DIENST IN OM HET RESULTAAT TE REMEDIËREN]. Deze [...] helpt om [VOEG IN WAT DE DIENST ZAL DOEN en HOE zij de dienst kunnen aanvragen]

**Wat kunt u doen.**

Naast onze voorgestelde diensten, raden wij u aan:

* [VOEG AANBEVELING IN].
* [VOEG AANBEVELING IN].
* een goede beveiliging van uw gegevens te waarborgen door ervoor te zorgen dat uw computer een antivirusbescherming heeft en dat deze up-to-date is, door uw wachtwoorden regelmatig bij te werken en door ervoor te zorgen dat uw wachtwoorden complex en uniek zijn.
* bijzondere aandacht te besteden aan e-mails waarin om persoonsgegevens, financiële informatie of rijksregisternummers wordt gevraagd. Deel geen rijksregisternummers of andere persoonsgegevens met onbekenden.
* wees altijd waakzaam voor oplichting door phishingscams. Phishingscams bestaan uit frauduleuze (d.w.z. valse of ‘gespoofte’) e-mailberichten die afkomstig lijken te zijn van legitieme bronnen en moedigen u aan om (i) op een link te klikken of een bijlage te openen waarmee malware op uw computer wordt gedownload, of (ii) bepaalde soorten informatie aan een onbekende derde te verstrekken. U kunt bijvoorbeeld een e-mail ontvangen die u instructies geeft om informatie, zoals uw gebruikersnaam en wachtwoord, in te voeren op een onbevoegde website zoals [WEBSITE] U kunt ook een e-mail ontvangen van een bron die legitiem lijkt, maar op de een of andere manier niet correct is. Een e-mail kan ook een phishingscam zijn als er bepaalde anomalieën zijn, zoals spelfouten of vreemde formuleringen.

Stuur verdachte e-mails altijd door naar [VOEG E-MAILADRES VAN IT SECURITY IN] voordat u klikt op links, bijlagen opent of op enige manier antwoordt.

**Voor meer informatie.**

We betreuren oprecht dat dit incident zich heeft voorgedaan en zullen verder [HERHAAL DE STAPPEN DIE WORDEN GENOMEN ALS REPONS OP HET INCIDENT] om ervoor te zorgen dat een gelijkaardig incident zich nooit meer kan voordoen bij [Bedrijf]

Als u vragen hebt, neem dan gerust contact op met [VOEG TITEL EN FUNCTIE VAN DE VERANTWOORDELIJKE PERSOON IN DIE DIENST DOET ALS FUNCTIONARIS VOOR GEGEVENSBESCHERMING OF CHIEF PRIVACY OFFICER] voor meer informatie over deze kwestie:

E-mail: [VOEG IN]

Telefoon: [VOEG IN]

Adres: [VOEG IN]

Met vriendelijke groeten,

[VOEG NAAM IN]

[VOEG TITEL IN]

1. **Melding aan de gegevensbeschermingsautoriteit**

Verschillende gegevensbeschermingsautoriteiten hebben online meldingsformulieren om een inbreuk in verband met persoonsgegevens te melden, zodat dit formulier niet nodig is. Bovendien zijn de onderstaande richtlijnen voor een dergelijke melding gebaseerd op de wetgeving inzake gegevensbescherming die van toepassing is op de lidstaten van de Europese Unie, namelijk de Algemene Verordening Gegevensbescherming (‘AVG’).

De sjabloon van de melding aan de toezichthoudende autoriteit moet minimaal de volgende informatie bevatten:

(a) een beschrijving van de aard van de inbreuk in verband met persoonsgegevens, inclusief, waar mogelijk, de categorieën en het geschatte aantal betrokkenen en de categorieën en het geschatte aantal betroffen bestanden met persoonsgegevens;

(b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen (bv. er zou voorgesteld worden om hier de compliance manager op te nemen);

(c) beschrijf de mogelijke gevolgen van de inbreuk in verband met persoonsgegevens;

(d) beschrijf welke maatregelen de verwerkingsverantwoordelijke heeft genomen of zal nemen om de inbreuk in verband met persoonsgegevens aan te pakken, inclusief, in voorkomend geval, maatregelen om de mogelijke negatieve gevolgen ervan te beperken.