Vragenlijst meldformulier datalekken

**In dit document vindt u de vragen uit het online** [**meldformulier datalekken**](https://datalekken.autoriteitpersoonsgegevens.nl/) **van de Autoriteit Persoonsgegevens (AP). Dit document helpt u om vóór het invullen van het online formulier de vragen alvast in te zien. Zo kunt u de benodigde informatie alvast verzamelen. Daarnaast kan de vragenlijst uw organisatie helpen om een stappenplan op te stellen waarmee u een (toekomstig) datalek zo tijdig en volledig mogelijk kunt melden.**

*Versie 1.1, augustus 2022*

## Disclaimer

U kunt geen rechten ontlenen aan dit document. De AP kan dit document tussentijds wijzigen. De laatste versie vindt u op de website van de AP.

**Let op: u kunt dit document niet gebruiken om een datalekmelding per post of e-mail aan de AP te sturen. De AP accepteert alleen datalekmeldingen via het online meldformulier datalekken.**

## Welke informatie heeft u (mogelijk) nodig bij het melden van een datalek?

Deze informatie heeft u altijd nodig:

* contactgegevens van de persoon die de AP kan benaderen bij vragen;
* contactgegevens van uw functionaris voor de gegevensbescherming (FG) (indien van toepassing);
* correspondentie over de ontdekking van het datalek;
* verwerkingsregister (artikel 30 AVG);
* datalekkenregister (artikel 33, lid 5 AVG);
* de getroffen maatregelen om het datalek te beëindigen;
* de getroffen maatregelen om het datalek in de toekomst te voorkomen;
* de maatregelen die u al voor het datalek had getroffen;
* data protection impact assessment (DPIA) (indien van toepassing).

Indien sprake is geweest van een hacking- of malware-incident of ander incident waarbij (extern) onderzoek heeft plaatsgevonden:

* het onderzoeksrapport naar aanleiding van de inbreuk.

Als u gebruikmaakt van een derde partij om persoonsgegevens te verwerken:

* verwerkersovereenkomst;
* andere overeenkomsten, zoals een samenwerkingsovereenkomst.

Als u de betrokkenen (de getroffen personen) moet informeren:

* correspondentie aan de betrokkenen.

## Onderzoek bij hacking, malware (bijv. ransomware) en/of phishing

Meldt u een datalek aan de AP als gevolg van hacking, malware (bijv. ransomware) en/of phishing? Dan verwacht de AP dat u zo snel mogelijk onderzoek doet of laat doen naar de omvang van het incident. Het is immers mogelijk dat kwaadwillende hackers op minder zichtbare delen van uw netwerk en/of systemen malware en andere wijzigingen hebben toegepast, waarmee ze bijvoorbeeld op een later moment weer toegang kunnen krijgen tot uw netwerk. Bovendien kunt u zonder het uitvoeren van onderzoek geen uitsluitsel krijgen over de vraag of persoonsgegevens door derden zijn ingezien, gekopieerd/gestolen of veranderd. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:

* Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?
* Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?
* Zijn er loggegevens beschikbaar en zo ja, kunt u met die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien?

## Documentatieplicht - datalekkenregister

Het melden van een datalek bij de AP is slechts een onderdeel van de meldplicht datalekken. Daarnaast moet u een register bijhouden waarin u alle datalekken registreert die binnen uw organisatie plaatsvinden. Dus ook de datalekken die u niet aan de AP heeft gemeld omdat dat niet nodig was. Neem in het register in ieder geval de volgende informatie op:

* de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegevens het gaat;
* de gevolgen van het datalek;
* de maatregelen die u heeft getroffen om het lek te dichten en om herhaling te voorkomen.

Het is aan te raden om ook aan te geven waarom u een datalek wel of niet heeft gemeld aan de AP en de betrokkenen. Maar dit is niet verplicht.

## Vragenlijst meldformulier datalekken

[**1. Introductie** 4](#_Toc92275374)

[**2. Internationale aspecten** 6](#_Toc92275375)

[**3. De verwerkingsverantwoordelijke** 8](#_Toc92275376)

[**4. Tijdlijn** 10](#_Toc92275377)

[**5. Gegevens over de inbreuk** 11](#_Toc92275378)

[**6. Welke persoonsgegevens** 16](#_Toc92275379)

[**7. Getroffen personen** 19](#_Toc92275380)

[**8. Maatregelen vooraf** 20](#_Toc92275381)

[**9. Gevolgen** 21](#_Toc92275382)

[**10. Vervolgacties** 23](#_Toc92275383)

[**11. Verzenden** 28](#_Toc92275384)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. Introductie** | **Een nieuwe melding doen van een inbreuk**  **1.1 Wat voor soort melding wilt u doen?**   * Ik wil één inbreuk melden (reguliere melding) [= door naar 1.2] * Ik wil meerdere gelijksoortige inbreuken, als gevolg van een grootschalige postverzending, tegelijk melden (bulkmelding) [= door naar 1.1.1]   **1.1.1. Heeft uw organisatie uitdrukkelijke schriftelijke toestemming ontvangen van de AP om inbreuken in bulk te melden?**   * Ja [=door naar 1.1.2] * Nee [EINDE FORMULIER]  |  | | --- | | Op dit moment loopt er een pilot waarbij alleen pensioenfondsen, verzekeraars en banken inbreuken in bulk mogen melden. Het is op dit moment niet mogelijk om toestemming te krijgen om bulkmeldingen in te dienen. Zodra dit wel kan, staat dit op de website van de AP. |   **1.1.2 Geef het aantal inbreuken aan dat u bij de AP in bulk wilt melden:**  [open veld]   |  | | --- | | Geef onder vraag 5.3 “Beschrijving van het incident” duidelijk aan dat het gaat om een bulkmelding, en geef aan om hoeveel poststukken het gaat. Controleer verder of u aan alle door de AP gestelde voorwaarden voor het doen van een bulkmelding heeft voldaan, voordat u de melding verstuurt. |   **1.2 Meldplicht AVG, Tw, Wjsg of Wpg**  **Op grond van welke wettelijke bepaling doet u deze melding?**   * Algemene verordening gegevensbescherming (AVG) * Telecommunicatiewet (Tw) * Wet justitiële en strafvorderlijke gegevens (Wjsg) * Wet politiegegevens (Wpg)  |  | | --- | | De meldplicht datalekken is in vier wetten opgenomen. In de meeste gevallen zult u een melding doen onder de AVG. Alleen wanneer u een telecommunicatieaanbieder bent of u op grond van de Wjsg of de Wpg persoonsgegevens verwerkt, kan dat anders zijn. |   **1.3 Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen ?**   * Ja, namelijk: Meerdere opties zijn mogelijk. * Autoriteit Financiële Markten (AFM) * Agentschap Telecom (AT) * De Nederlandsche Bank (DNB) * Inspectie Gezondheidszorg en Jeugd (IGJ) * Inspectie Leefomgeving en Transport (ILT) * Inspectie voor het Onderwijs * Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) * Onderzoeksraad voor Veiligheid (OVV) * Andere toezichthouder, namelijk [open veld] * Nee |
| **2. Internationale aspecten** | **2.1 Grensoverschrijdende inbreuk**  **2.1.1 Heeft de inbreuk gevolgen voor personen in meerdere landen?**   * Ja [= door naar 2.1.2] * Nee [= door naar 3]  |  | | --- | | Wanneer u persoonsgegevens verwerkt in meer dan één land of wanneer de verwerking schadelijke gevolgen kan hebben voor personen in meer dan één land, is het mogelijk dat u de inbreuk bij meer dan één toezichthouder moet melden. Twijfelt u of u de inbreuk bij de AP of bij een toezichthouder uit een ander Europees land moet melden? Dan kunt u gebruik maken van het “[Stroomschema identificatie leidende toezichthouder](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stroomschema_leidende_toezichthouder.pdf)”. Zie daarnaast de [Q&A](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/een-loketmechanisme-onestopshop#wanneer-zijn-de-gegevensverwerkingen-van-mijn-organisatie-grensoverschrijdend-5783) voor meer informatie. |   **2.1.2 Bevindt de hoofdvestiging of de enige vestiging van uw organisatie zich in Nederland?**   * Ja [= door naar 2.1.3] * Nee [= door naar 2.1.3]  |  | | --- | | De AP is de leidende toezichthouder wanneer de hoofdvestiging of de enige vestiging van uw organisatie zich in Nederland bevindt. |   **2.1.3 Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke landen gaat het dan?**  [lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven]  **2.2 Bevoegde toezichthouders in andere EU-lidstaten**  **2.2.1 Heeft uw organisatie de inbreuk gemeld bij andere privacytoezichthouders?**   * Nee [= door naar 2.2.2] * Ja [= door naar 2.2.1.1]   **2.2.1.1 Geef aan in welk(e) land(en) u de inbreuk aan de privacytoezichthouder heeft gemeld.** Meerdere opties zijn mogelijk.  [lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven]  **2.2.2 Gaat uw organisatie de inbreuk nog melden bij andere privacytoezichthouders?**   * Nee [= door naar 3] * Ja [= door naar 2.2.2.1]   **2.2.2.1 Geef aan in welk(e) land(en) u de inbreuk aan de privacytoezichthouder gaat melden.** Meerdere opties zijn mogelijk.  [lijst met EU landen + mogelijkheid andere landen op te geven + optie om aantal betrokkenen op te geven] |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **3. De verwerkings­verantwoordelijke** | | **3.1 Contactgegevens**  **3.1.1. Over welke organisatie of welk bedrijf gaat het?**   |  |  | | --- | --- | | Registratienummer van de FG | [open veld] [optioneel] | | KvK-nummer | [open veld] [optioneel] | | Naam van het bedrijf of de organisatie | [open veld] | | Adres | [open veld] | | Postcode | [open veld] | | Plaats | [open veld] |   **3.1.2 In welke sector is de organisatie of het bedrijf actief?**  [Lijst met sectoren]   |  | | --- | | Weet u niet zeker binnen welke sector u actief bent, controleer dan binnen welke SBI u bij de Kamer van Koophandel geregistreerd staat of selecteer de sector die het dichtst bij uw economische activiteiten in de buurt komt. |   **3.2 Gegevens melder en contactpersoon**  **3.2.1 Wie meldt de inbreuk?**   |  |  | | --- | --- | | Naam | [open veld] | | Functie | [open veld] | | E-mailadres | [open veld] | | Telefoonnummer | [open veld] | | Tweede telefoonnummer | [open veld] [Optioneel] |  |  | | --- | | Dit dient een direct telefoonnummer te zijn en geen algemeen telefoonnummer |   **3.2.2 Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?**   * Ja [= door naar 3.3] * Nee [velden invullen en daarna door naar 3.3]  |  |  | | --- | --- | | Naam contactpersoon | [open veld] | | Functie contactpersoon | [open veld] | | E-mailadres contactpersoon | [open veld] | | Telefoonnummer contactpersoon | [open veld] | | Tweede telefoonnummer | [open veld] [Optioneel] |  |  | | --- | | De contactpersoon dient daags na de melding goed bereikbaar te zijn tijdens kantooruren om eventuele vragen van de AP over de inbreuk te kunnen beantwoorden. |   **3.3 Andere organisaties**  **3.3.1 Waren er andere organisaties betrokken bij de inbreuk?**   * Ja [= door naar 3.3.2] * Nee [= door naar 4]  |  | | --- | | Een organisatie is betrokken bij de inbreuk als deze een rol heeft gehad bij het ontstaan van de inbreuk. |   **3.3.2 Geef aan welke andere organisaties betrokken waren bij de inbreuk?**   |  |  |  | | --- | --- | --- | | Naam | Op welke wijze betrokken | Toelichting (optioneel) | | Organisatie A | bijvoorbeeld verwerker |  | | Organisatie B |  |  | | + Voeg nog een organisatie toe |  |  | |
| **4. Tijdlijn** | **4.1. Duurt de inbreuk op dit moment nog voort?**   * Ja [=door naar 4.1.1] * Nee [=door naar 4.1.1 + 4.1.2] * Onbekend [=door naar 4.1.1]   **4.1.1 (Mogelijke) startdatum van de inbreuk** [datumveld]  **4.1.2 (Mogelijke) einddatum van de inbreuk** [datumveld]  **4.2 Wanneer is het incident ontdekt?** [datumveld]  **4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt**  [open veld]  **4.4 Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?**   * Ja [=door naar 5, tenzij later dan 72 uur na de ontdekkingsdatum dan door naar 4.5] * Nee [=door naar 4.4.1]  |  | | --- | | Met het krijgen van kennis van een inbreuk wordt bedoeld dat u op basis van objectieve factoren heeft kunnen aannemen dat het aannemelijk is dat een datalek zich heeft voorgedaan. Dit hoeft niet het moment te zijn waarop u het datalek heeft ontdekt. **Let op**: Dit kan niet het moment zijn waarop het incident bij de FG werd gemeld. De FG is niet verantwoordelijk voor de verplichtingen die de meldplicht datalekken met zich mee brengt. Dit betekent dat de AP dit niet als gerechtvaardigde reden beschouwd waarom de melding te laat is ingediend. |   **4.4.1 Wanneer heeft u kennis gekregen van de inbreuk?** [datumveld]  Als de inbreuk later dan 72 uur na kennisname wordt gemeld moet de volgende vraag beantwoord worden:  **4.5 Beschrijf hieronder waarom u de inbreuk later dan 72 uur na ontdekking meldt:**  [open veld] | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **5. Gegevens over de inbreuk** | **5.1 Aard van de inbreuk**  Meerdere opties zijn mogelijk.   |  | | --- | | Bij een incident kan sprake zijn van één of meerdere type inbreuken die gaan over de vertrouwelijkheid, de beschikbaarheid en de integriteit van de persoonsgegevens. Een voorbeeld hiervan is wanneer u geconfronteerd wordt met ransomware (gijzelsoftware). Om een bestand te versleutelen / gijzelen dient de malafide software de bestanden eerst te openen om deze vervolgens te kunnen versleutelen. Hierdoor is zowel sprake van een inbreuk op de vertrouwelijkheid / ingezien door onbevoegden als sprake van een inbreuk op de beschikbaarheid. Kijk voor meer informatie in onze [Q&A](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#kunnen-bestanden-zijn-versleuteld-zonder-eerst-geopend-te-zijn-5691). |  * Peroonsgegevens (mogelijk) ingezien door onbevoegden  |  | | --- | | Onder “ingezien” wordt ook bedoeld dat er sprake is (geweest) van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. |  * Persoonsgegevens ongeoorloofd of onopzettelijk gewijzigd * Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd) * Persoonsgegevens tijdelijk niet beschikbaar  |  | | --- | | Het moet gaan om onopzettelijk of ongeoorloofd verlies van toegang tot persoonsgegevens óf een onopzettelijke of ongeoorloofde vernietiging van persoonsgegevens. Hiervan kan ook sprake zijn als u (tijdelijk) geen gebruik kunt maken van de persoonsgegevens die noodzakelijk zijn voor de verwerkingsdoeleinden. |   **5.2 Aard van het incident**  **Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?** Slechts één optie is mogelijk.   * E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)   **5.2.1.Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?**   * Ja [= door naar 5.3] * Nee [= door naar 5.3] * De verkeerde ontvanger heeft niet gereageerd [= door naar 5.3] * E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc [= door naar 5.3] * Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)   **5.2.2. Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?**   * Ja [= door naar 5.3] * Nee [= door naar 5.3] * De verkeerde ontvanger heeft niet gereageerd [= door naar 5.3] * Brief of postpakket met persoonsgegevens geopend retour ontvangen [= door naar 5.3] * Brief of postpakket met persoonsgegevens kwijtgeraakt [= door naar 5.3] * Autorisatie(s) van medewerker(s) verkeerd ingesteld. [= door naar 5.3]  |  | | --- | | Dit incident heeft betrekking op de situatie waarbij de toegang- of leesrechten van een gebruiker niet of abusievelijk zijn aangepast, waardoor een gebruiker meer mogelijkheden in het systeem heeft dan zou moeten. Bijvoorbeeld: een autorisatierol is bij functiewijziging niet goed doorgevoerd. |  * Netwerkmappen of -locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie. [= door naar 5.3]  |  | | --- | | Dit heeft betrekking op het systeem, waarbij een gedeelde map, locatie of applicatie verkeerd is ingesteld en daardoor voor onbevoegde personen is in te zien. Bijvoorbeeld: Een map met personeelsgegevens was toegankelijk voor elke medewerker. |  * Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen [= door naar 5.3] * Persoonsgegevens per ongeluk gepubliceerd [= door naar 5.3] * Hacking, malware (bijv. ransomware) en/of phishing Meerdere opties zijn mogelijk  |  | | --- | | De AP adviseert u tevens aangifte te doen bij de Politie wegens onder andere computervredebreuk en/of computersabotage. Door aangifte te doen kan de politie in overleg met het Openbaar Ministerie (OM) besluiten om een onderzoek te starten en helpt u het OM bij het in kaart brengen van criminaliteit. Hiermee kan de politie strafbare feiten opsporen en meer slachtoffers voorkomen. Kijk voor meer informatie op [www.nomoreransom.org](http://www.nomoreransom.org). |  * Phishing [= door naar 5.2.3]  |  | | --- | | Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben informatie van mensen te ontfutselen. Met deze informatie kunnen criminelen toegang krijgen tot (bedrijfs-)netwerken en fraude plegen, bijvoorbeeld bankfraude of identiteitsfraude. |  * Ransomware [= door naar 5.2.3]  |  | | --- | | Ransomware is kwaadaardige software die een computer of bestanden gijzelt. In de meeste gevallen wordt daarna betaling geëist. |  * Ander type hacking en/of malware [= door naar 5.2.3]  |  | | --- | | Hieronder kunnen alle activiteiten vallen waarbij onrechtmatig toegang is verschaft tot persoonsgegevens of waarbij persoonsgegevens op een andere wijze onrechtmatig zijn aangetast. |  |  | | --- | | * + Ransomware kan het hele systeem en alle gekoppelde bestanden raken. U kunt bij ransomware zonder (digitaal forensisch) onderzoek uit te voeren er niet van uit gaan dat de inbreuk beperkt is gebleven tot het zichtbaar besmette bestand of systeem.   + Een geslaagde phishing-actie, waarbij e-mailadres en wachtwoord zijn bemachtigd, kan ertoe leiden dat hackers toegang krijgen tot mailboxen, netwerken en systemen. In het geval van mailboxen is het mogelijk dat ook de e-mails in een mailbox zijn getroffen. Bij phishing kunnen dus niet alleen de contactpersonen in het adresboek van het e-mailaccount getroffen zijn, maar ook de personen van wie er e-mails in mailbox zijn opgeslagen. |   **5.2.3. Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van de inbreuk?** [= door naar 5.3]   * Ja, het onderzoek loopt  |  | | --- | | Zodra het onderzoek is afgerond, moet u een vervolgmelding doen bij de AP.  De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:   * + Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?   + Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?   + Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien? |  * Ja, het onderzoek is afgerond [= door naar 5.2.3.1]   **5.2.3.1. Upload hier de rapportage van het onderzoek naar de inbreuk**  [UPLOAD-knop] [optioneel]   * Nee, het onderzoek is nog niet gestart  |  | | --- | | De AP verwacht dat u zo snel mogelijk onderzoek (laat) doen naar de aard en de omvang van de inbreuk. U moet binnen 4 weken een vervolgmelding doen met de stand van zaken. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:   * + Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?   + Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?   + Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien? |  * Nee, er wordt geen onderzoek verricht  |  | | --- | | Zonder onderzoek zal de onzekerheid over de omvang van de besmetting echter blijven bestaan. Dit betekent dat u niet redelijkerwijs kunt uitsluiten dat persoonsgegevens door een derde zijn ingezien, gekopieerd, gestolen of veranderd. De AP verwacht dat u zo snel mogelijk onderzoek (laat) doen naar de aard en de omvang van de inbreuk. De AP verwacht dat u in ieder geval het volgende bij uw onderzoek betrekt:   * + Is er toegang geweest tot de persoonsgegevens, bijvoorbeeld tot e-mails in een mailbox of de inhoud van een database?   + Zijn deze persoonsgegevens gekopieerd, ingezien of anderszins verzonden naar de hackers?   + Zijn er loggegevens beschikbaar en, zo ja, kan u aan de hand van die loggegevens uitsluiten dat persoonsgegevens zijn gekopieerd of ingezien? |   **5.2.3.2 Licht toe waarom u geen onderzoek verricht.**  [open veld]   * Persoonsgegevens van verkeerde klant getoond in klantportaal * Persoonsgegevens toegevoegd aan het verkeerde dossier * Persoonsgegevens bij oud papier gezet * Persoonsgegevens door storing (tijdelijk) niet beschikbaar * Overig, namelijk: [open veld]   **5.3 Beschrijving van het incident**  **Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest**  [open veld]  **5.4 Indien beschikbaar: upload hier relevante ondersteunende documentatie bij uw melding.**  Let op dat u geen persoonsgegevens opneemt in de bestanden als dat niet noodzakelijk is.  [UPLOAD-knop] [optioneel] |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **6. Welke persoonsgegevens** | **6.1 Persoonsgegevens in het algemeen** Meerdere opties zijn mogelijk  ☐ Naam  ☐ Geslacht  ☐ Geboortedatum en/of leeftijd  ☐ Burgerservicenummer (BSN)  ☐ Contactgegevens  ☐ Adres en woonplaats  ☐ E-mailadres  ☐ Telefoonnummer  ☐ Toegangs- of identificatiegegevens   |  | | --- | | Bijvoorbeeld gebruikersnamen en wachtwoorden |     ☐ Financiële gegevens  ☐ Bankrekeningnummer / IBAN  ☐ Creditcardgegevens  ☐ Gegevens over (problematische) schulden  ☐ Gegevens over uitkering en/of schulden  ☐ Andere financiële gegevens, namelijk:[open veld]  ☐ (Kopieën van) paspoorten of andere legitimatiebewijzen  ☐ Locatiegegevens   |  | | --- | | Geen NAW-gegevens. Hiermee worden gegevens bedoeld om de locatie van een persoon te bepalen of te kunnen volgen, bijv. GPS-gegevens, zendmastgegevens. |   ☐ Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen   |  | | --- | | Ook indirect kan sprake zijn van een strafrechtelijk persoonsgegeven, bijvoorbeeld afgeleid uit het ontwerp of logo van een envelop afkomstig van de reclassering of het Openbaar Ministerie. |   ☐ Anders, namelijk: [open veld]  ☐ Onbekend   |  | | --- | | Indien onbekend is geselecteerd:  U moet binnen 4 weken een vervolgmelding indienen, waarin u aangeeft welke persoonsgegevens bij het datalek betrokken zijn. |   **6.2 Bijzondere categorieën van persoonsgegevens**   |  | | --- | | Een bijzonder persoonsgegeven kan ook indirect blijken uit feiten en omstandigheden van de situatie. Denk bijvoorbeeld aan de envelop die gebruikt is of het bijzondere kenmerk van uw organisatie, bijvoorbeeld een kerk, vakbond, LHBTQ-vereniging, een GGZ-instelling of specialistische zorg (bijv. oncologie). |  * Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt * Persoonsgegevens waaruit iemands politieke opvattingen blijken * Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken * Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt * Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid * Gegevens over iemands gezondheid * Genetische gegevens * Biometrische gegevens (bijvoorbeeld: vingerafdruk of irisscan)  |  | | --- | | Dit zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon. Op grond hiervan is eenduidige identificatie van die persoon mogelijk. Of wordt zijn/haar identiteit bevestigd. |   **6.3 Hoeveelheid persoonsgegevens**  **6.3.1 Geef (eventueel bij benadering) aan hoeveel gegevensrecords (gegevensregisters) zijn getroffen door de inbreuk**  [open veld]     |  | | --- | | Met een gegevensrecord (artikel 33, lid 3, sub a AVG) wordt bedoeld: de registratie van informatie over een gebeurtenis of over een persoon. Het begrip laat zich het beste uitleggen aan de hand voorbeelden:   1. Elke regel in een database vormt één gegevensrecord. Dit kan een database zijn met alle geplaatste orders, maar kan ook een database zijn met alle klantgegevens (CRM). 100 klanten in een CRM systeem vormen 100 records. Als elke klant 5 orders heeft geplaatst bij dat bedrijf staan er 500 gegevensrecords als order opgenomen in de orderdatabase; 2. Elke regel in een logboek vormt één gegevensrecord. In een medisch dossier wordt bijvoorbeeld bijgehouden wie wanneer inzage heeft gehad en handelingen heeft verricht in het dossier. Als iemand een dossier heeft geopend en één ding heeft aangepast, dan kunnen er minstens drie regels aangemaakt zijn (openen dossier (1), wijzigen informatie (2), sluiten dossier (3)); 3. Een brief vormt één gegevensrecord. De dagtekening, gegevens van de geadresseerde en afzender staan als informatie opgenomen in de brief; 4. Een e-mail vormt één gegevensrecord. De verzenddatum en –tijdstip, de geadresseerde en de verzender staan in de mail; 5. Een paspoort vormt één gegevensrecord. Op een paspoort staat informatie opgenomen over een persoon, zoals naam, geboortedatum, nationaliteit, BSN, documentnummer van het paspoort en de stempels van de douane van de landen waar iemand is geweest; 6. Een (papieren) dossier van een persoon vormt ook een record, omdat daar informatie is opgeslagen over een persoon.   Het is mogelijk dat er meerdere soorten gegevensrecords zijn getroffen bij een inbreuk, omdat bijvoorbeeld het gehele netwerk is getroffen, waardoor zowel CRM als HR gegevens zijn getroffen. In de volgende vraag kunt u een toelichting geven op de getroffen gegevensrecords. Als het aantal gegevensrecords te groot is of als u niet weet hoeveel persoonsgegevensregisters zijn getroffen, voer dan “1” in en licht het aantal toe bij de volgende vraag. Zie voor meer informatie de Q&A. |   **Geef een toelichting op bovengenoemd aantal:**  [open veld]   |  | | --- | | Hier kunt u een nadere toelichting geven op het aantal en soort getroffen gegevensrecords . Aan de hand van uw toelichting kan de AP een beter of genuanceerder beeld krijgen van het incident. U kunt bijvoorbeeld aangeven of er één of meerdere databases zijn getroffen of dat de inbreuk is beperkt tot een brief of een dossier. | |

|  |  |  |
| --- | --- | --- |
| **7. Getroffen personen** | **7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?** Meerdere opties zijn mogelijk.   * Werknemers * Klanten (huidig en potentieel) * Leerlingen of studenten * Patiënten * Minderjarigen * Personen uit andere kwetsbare groepen * Anders, namelijk: [open veld]  |  | | --- | | Met “betrokkene” wordt hier bedoeld de persoon van wie de persoonsgegevens zijn getroffen door de inbreuk. |   **7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.**  [open veld]  **7.3 Is het exacte aantal betrokkenen bekend?**   * Ja   **7.3.1 Het exacte aantal is**: [open veld]   * Nee   **7.3.2 Het minimum aantal betrokkenen is:** [open veld]  **7.3.3 Het maximum aantal betrokkenen is:** [open veld] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8. Maatregelen vooraf** | **8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?** Meerdere opties zijn mogelijk.   * Ja, namelijk: versleuteld (encryptie)   **8.1.1 Welke versleutelingstechniek heeft u toegepast (indien bekend)?**  [open veld+ optioneel]   |  | | --- | | Probeer waar mogelijk ook details te geven, zoals het aantal bits van de gebruikte sleutel en de standaard (bijvoorbeeld AES-256). Let op: indien een laptop of andere drager beveiligd is met een wachtwoord betekent dat niet altijd dat de gegevens op de drager zijn versleuteld en onder “versleuteld” wordt niet bedoeld: versleuteld door een ransomware aanval. |  * Ja, namelijk gehasht   **8.1.2 Welke hashingtechniek heeft u toegepast (indien bekend)?**  [open veld+ optioneel]   |  | | --- | | Denk bijvoorbeeld aan MD5, SHA-256, bcrypt, of een andere cryptografische hashfunctie. Geef hierbij ook aan of er gebruik gemaakt is van een salt. |  * Ja, namelijk: op een andere manier onbegrijpelijk of ontoegankelijk gemaakt   **8.1.3 Op welke manier waren de gegevens onbegrijpelijk of ontoegankelijk gemaakt (indien bekend)?**  [open veld+ optioneel]   |  | | --- | | Denk hierbij aan standaard versleutelde soft- of hardware of andere beveiligingsmethoden |  * Nee [= direct door naar 9]   **8.2 Als de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt waren, om welk deel gaat dat dan?**   * Alle gegevens waren vooraf onbegrijpelijk of ontoegankelijk gemaakt * Een deel van de gegevens was onbegrijpelijk of ontoegankelijk gemaakt, namelijk: [open veld] |

|  |  |  |  |
| --- | --- | --- | --- |
| **9. Gevolgen** | **9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.** Meerdere opties zijn mogelijk.   * Onbevoegden hebben kennis kunnen nemen van de gegevens * De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt * Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt * Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties * Een essentiële dienst kan tijdelijk niet meer worden verleend aan degenen van wie gegevens zijn gelekt * Een essentiële dienst kan permanent niet meer worden verleend aan degenen van wie gegevens zijn gelekt * Anders, namelijk: [open veld]      |  | | --- | | Hiermee wordt bedoeld welk effect de inbreuk mogelijk heeft op uw organisatie en de verwerking van persoonsgegevens binnen uw organisatie. |   **9.2 (Mogelijke) gevolgen voor de betrokkene(n)** Meerdere opties zijn mogelijk.   * Discriminatie of uitsluiting * Identiteitsdiefstal of -fraude * Financieel verlies * Reputatieschade * Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens * Ongeoorloofde ongedaanmaking van pseudonimisering * Betrokkenen kunnen bijvoorbeeld (de verwerking van) hun persoonsgegevens niet inzien of op verzoek laten verwijderen (Uitoefening van rechten) * Betrokkenen verliezen het overzicht van welke organisaties hun persoonsgegevens verwerken en worden verhinderd controle uit te oefenen * Anders, namelijk: [open veld]   **9.3 Inschatting risico**  **Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)**   * Verwaarloosbaar * Beperkt * Aanzienlijk * Zeer groot   **Licht uw keuze toe:**  [open veld]   |  | | --- | | Er zijn in ieder geval 7 factoren waar u rekening mee dient te houden:   1. Welk incident heeft plaatsgevonden? 2. Hoeveel persoonsgegevens en welke soort persoonsgegevens zijn getroffen én hoe gevoelig zijn de persoonsgegevens in de context waarin de persoonsgegevens worden verwerkt? 3. Hoe makkelijk zijn de gegevens te koppelen aan een natuurlijk persoon? 4. Hoe ernstig kunnen de hierboven aangegeven eventuele gevolgen zijn? 5. Behoort de betrokkene tot een kwetsbare groep? 6. Heeft u uw organisatie een bijzondere positie (zoals een ziekenhuis, een bank, een (bijzondere) school) 7. Wat is de grootte van de groep betrokkenen?   Daarnaast kunt u specifieke feiten en omstandigheden meenemen waardoor het risico voor de betrokkenen verhoogd of verlaag worden. Raadpleeg Richtsnoeren voor de melding van datalekken vanaf pagina 27 voor meer informatie. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **10. Vervolgacties** | **10.1 Informeren van de betrokkene(n)**  **10.1.1. Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?**   * Ja [= door naar 10.1.3] * Nee [= door naar 10.1.2]   **10.1.2 Gaat u de inbreuk nog melden aan de betrokkene(n)?**   * Ja [= door naar 10.1.4] * Nee [direct door naar 10.2] * Nog niet bekend [direct door naar 10.2]  |  | | --- | | Let op, u moet er vanuit gaan dat u de inbreuk moet melden aan de betrokkene(n) als het gaat om de volgende persoonsgegevens:   * bijzondere persoonsgegevens * strafrechtelijke persoonsgegevens * kopieën van identiteitsbewijzen en/of paspoorten * combinatie van BSN, naam en geboortedatum * persoonsgegevens van mensen een kwetsbare groep * veel persoonsgegevens of persoonsgegevens van veel betrokkenen   En/of de inbreuk kan leiden tot:   * discriminatie * identiteitsdiefstal of –fraude * financiële verliezen * reputatieschade * doorbreking van beroepsgeheim   Zie ook: de [Guidelines meldplicht datalekken.](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf)  **Let op bij phishing**  Indien u een phishing incident meldt ten aanzien van een e-mailaccount is het mogelijk dat u twee groepen betrokkenen moet informeren, namelijk degenen wiens contactgegevens in het adresboek in de e-mailbox stonden en de degenen wiens (bijzondere of gevoelige) persoonsgegevens in e-mails in de e-mailbox waren opgeslagen, bijvoorbeeld in een bijlage. |   **10.1.3 Aan hoeveel personen heeft u de inbreuk gemeld?**  [invoerveld]  **10.1.4 Aan hoeveel personen wilt u de inbreuk gaan melden?**  [invoerveld]   |  | | --- | | Let op: komt het door u opgegeven aantal betrokkenen dat u gaat informeren niet overeen met het aantal dat u bij vraag 7 heeft opgegeven? Dan vragen wij u dit nader toe te lichten.  **Let op bij phishing**  Indien u een phishing incident meldt ten aanzien van een e-mailaccount is het mogelijk dat u twee groepen betrokkenen moet informeren, namelijk degenen wiens contactgegevens in de e-mailbox stonden en de degenen wiens (bijzondere of gevoelige) persoonsgegevens in e-mails in de e-mailbox waren opgenomen, bijvoorbeeld in een bijlage. |   **10.1.5 Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?** [= door naar 10.1.7]  [datumveld]    **10.1.6 Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?** [= door naar 10.1.7]  [datumveld]  **10.1.7 Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld.** [= door naar 10.1.8]  [invoerveld]  **10.1.8 Wat is de inhoud van de melding aan de betrokkene(n)?** [= door naar 10.1.9]  [open veld]   |  | | --- | | U bent verplicht aan te geven:   * Wat er is gebeurd; * Wat de gevolgen zijn; * Welke maatregelen u heeft getroffen, en; * De naam en contactgegevens van de functionaris voor de gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen. |   **Optioneel: Upload hier een kopie van de tekst van deze kennisgeving**  [UPLOAD-knop]  **10.1.9 Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?** Meerdere opties zijn mogelijk.   * Telefonisch * Per brief * Per e-mail * Via een mededeling op de website * Via social media * Via een advertentie in de krant * Anders, namelijk: [open veld]      |  | | --- | | Indien alleen “Via een mededeling op de website” is aangekruist:  Een mededeling die beperkt blijft tot een algemene mededeling op uw website is over het algemeen geen effectief middel om een inbreuk aan een persoon mee te delen. De AP raadt u aan een middel te kiezen waarbij de kans dat de informatie naar behoren aan alle getroffen personen wordt meegedeeld, zo groot mogelijk is. Dat kan betekenen dat u verschillende communicatiemethoden gebruikt in plaats van één enkel contactkanaal. Bijvoorbeeld via een aanvullend persbericht, uw bedrijfsblog, en via de officiële social media accounts van uw organisatie. |   **10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)**  **10.2.1 Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?** Meerdere opties zijn mogelijk   * Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren   **10.2.1.1 Licht toe waarom het een onevenredige inspanning zou vergen om de betrokkenen op individuele basis te informeren.**  [open veld]   * De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene(n) achterwege te kunnen laten   **10.2.1.2. Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?**  [open veld]   * Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkene(n)   **10.2.1.2. Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?**  [open veld]   * Mijn organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht (uitzondering artikel 42 UAVG). * Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren. Namelijk:   [open veld]   |  | | --- | | De getroffen personen hoeven niet te worden geïnformeerd, indien dat noodzakelijk en evenredig is ter bescherming van:   * de nationale veiligheid; * landsverdediging; * de openbare veiligheid; * de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; * andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid; * de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures; * de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen; * een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g; * de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of de inning van civielrechtelijke vorderingen. |  * Andere reden(en), namelijk:   [open veld]  **10.3. Maatregelen om de inbreuk aan te pakken**  **10.3.1 Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?**   * Nee, want:   [open veld]   * Nog niet bekend [U bent verplicht een vervolgmelding te doen waarin u aangeeft welke maatregelen u heeft getroffen om de inbreuk te beëindigen.] * Ja, namelijk:   [open veld]   |  | | --- | | Bijvoorbeeld verzocht om vernietiging van de verkeerd bezorgde brief of e-mail te verwijderen, het controleren van de logging om een inbreuk uit te sluiten, het dichtzetten van het beveiligingslek, het aanpassen van de autorisatiestructuur / rechtenstructuur. |   **10.3.2 Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?**   * Nee, want:   [open veld]   * Nog niet bekend [U bent verplicht een vervolgmelding te doen waarin u aangeeft welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.] * Ja, namelijk:   [open veld]   |  | | --- | | Bijvoorbeeld het geven van bewustwordingstraining, het aanpassen van werkprocessen, het toepassen van versleuteling op mobiele gegevensdragers, zoals laptops en USB-sticks, of het implementeren van twee- of multifactor authenticatie (MFA) op mailaccounts of applicaties. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **11. Verzenden** | Is dit een voorlopige of een definitieve melding?   * Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig * Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk  |  | | --- | | Bent u nog bezig met onderzoek om de aard en omvang van de inbreuk vast te stellen? Dan vraagt de AP u om hier “nee” in te vullen en binnen 4 weken een vervolgmelding te doen waarin u de AP op de hoogte brengt van de voortgang of uitkomst van het onderzoek. |   **Datum vervolgmelding later dan 4 weken:**  **Geef aan wanneer u (uiterlijk) een vervolgmelding doet.**  [datumveld]   |  | | --- | | De AP vraagt u binnen 4 weken na de eerste melding een vervolgmelding te doen waarin u een update geeft over de stand van zaken. Mocht u langer dan 4 weken nodig hebben, dan moet u dit motiveren.  Heeft de AP binnen 4 weken geen vervolgmelding ontvangen? Dan kan de AP contact met u opnemen. Doet u geen definitieve melding, dan kan u niet (volledig) aan uw meldplicht op grond van artikel 33 AVG hebben voldaan. De AP kan dan een nader onderzoek instellen. |  * Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen. * Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie   Privacyverklaring   * Ik ben op de hoogte van de inhoud van de [Privacyverklaring](https://autoriteitpersoonsgegevens.nl/nl/privacystatement-formulier-meldplicht-datalekken.) van de AP   **EINDE FORMULIER** |