Datum
9 december 2021

Versie
2.0

Toetsingskader datalekken

Aanleiding

De Algemene Verordening Gegevensbescherming (AVG) bevat grofweg drie verplichtingen ten aanzien van inbreuken in verband met persoonsgegevens (oftewel datalekken):

1. De AVG verplicht dat de verwerkingsverantwoordelijke een datalek zonder onredelijke vertraging en, uiterlijk 72 uur nadat hij er kennis van heeft genomen, meldt aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene(n). Indien de melding later dan 72 uur wordt gedaan, dient de vertraging gemotiveerd te worden.

2. De AVG verplicht dat wanneer het datalek een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene(n), de verwerkingsverantwoordelijke de betrokkene(n) onverwijld informeert over het datalek.

3. De AVG verplicht dat de verwerkingsverantwoordelijke alle datalekken documenteert, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

Doel

Het doel van dit toetsingskader is om een overzichtelijk kader te creëren waarmee (1) getoetst kan worden of er sprake is van een datalek, (2) de risico's van een datalek beoordeeld kunnen worden en (3) duidelijkheid gegeven wordt over het documenteren van datalekken.

Doelgroep

De doelgroep voor dit toetsingskader zijn de medewerkers van Bureau Gegevensbescherming die zijn belast met het beoordelen en documenteren van datalekken.

Leeswijzer

In dit toetsingskader is de beoordeling en behandeling van een datalek in vijf onderdelen uitgewerkt. Ook zijn er drie bijlagen met aanvullende informatie.

- Onderdeel 1: Vaststellen van een datalek
- Onderdeel 2: Risicobeoordeling
- Onderdeel 3: Melden aan de AP
- Onderdeel 4: Informeren van betrokkene(n)
- Onderdeel 5: Documentatieplicht

In bijlage 1 is een stroomschema opgenomen.
In bijlage 2 zijn vuistregels, betrouwbare ontvangers en praktijkvoorbeelden opgenomen.
In bijlage 3 worden richtsnoeren meegegeven voor het invullen van het meldformulier van de AP.

Bronnen

Naast dit Toetsingskader zijn er een aantal belangrijke bronnen die geraadpleegd kunnen worden bij het beoordelen en behandelen van een datalek. Dit zijn:

- De pagina Meldplicht datalekken op de website van de AP.
- De Richtsnoeren voor het melden van datalekken van de Werkgroep artikel 29.
- Het UWV datalekproces op DWU en de BG werkinstructie datalekken op de SharePoint van BG.

ONDERDEEL 1: Vaststellen van een datalek

Dit onderdeel behandelt het vaststellen van een datalek. Onderstaande vragen kunnen één voor één afgegaan worden voor het beoordelen of er sprake is van een datalek.

1.1. Is UWV verwerkingsverantwoordelijke voor de verwerking waarbij het beveiligingsincident is ontstaan?

UWV is verantwoordelijk voor een verwerking (verwerkingsverantwoordelijke) wanneer UWV feitelijk het doel en middelen van de verwerking bepaalt of door de wetgever is aangewezen als (gezamenlijke) verwerkingsverantwoordelijke.

Toelichting
UWV verwerkt voornamelijk persoonsgegevens om haar wettelijke taak uit te voeren (zoals het verstrekken van uitkeringen WW, WIA , re-integratie taken, etc.). Vindt er in dit proces een incident plaats, dan is UWV de verwerkingsverantwoordelijke.

Let op als er een andere organisatie betrokken is bij de gegevensverwerking, bijvoorbeeld een andere overheidsorganisatie. Dan moet er goed gekeken worden voor welke doeleinden en taken de verwerking van persoonsgegevens plaatsvond. Mogelijk is die andere partij verwerker en is UWV verwerkingsverantwoordelijke. Het kan ook voorkomen dat twee partijen gezamenlijk verwerkingsverantwoordelijke zijn. In dat geval moeten de partijen over de afhandeling van het datalek van te voren afspraken vastleggen. Indien er geen afspraken zijn vastgelegd dient JZ geraadpleegd te worden. Treedt UWV op als verwerker? De verwerkingsverantwoordelijke dient dan geïnformeerd te worden, waarna de behandeling van het incident wordt afgestemd.

Voorbeeld UWV verwerkingsverantwoordelijke voor datalek
Een arbeidsdeskundige rapportage (AD) wordt aan de verkeerde envelop toegevoegd en komt bij de verkeerde klant terecht. UWV is hier verwerkingsverantwoordelijke.

Voorbeeld UWV niet verwerkingsverantwoordelijke voor datalek
UWV stuurt een betalingsspecificatie met het logo van UWV naar een juiste schuldhulpverlener. De verwerking voor het versturen van de specificatie door UWV is hiermee afgerond. De schuldhulpverlener stuurt deze betalingsspecificatie vervolgens niet naar zijn cliënt, maar naar een onbevoegde derde. De schuldhulpverlener is de verwerkingsverantwoordelijke voor het verder doorsturen. Deze derde maakt melding van het datalek bij UWV. In deze situatie is de schuldhulpverlener verantwoordelijk voor het doorsturen en dus voor het datalek en stuurt UWV de melding van het datalek door naar de schuldhulpverlener.

1.2. Is er sprake van persoonsgegevens?

Er kan alleen sprake zijn van een datalek bij een inbreuk op *persoonsgegevens*.

Toelichting
Het begrip persoonsgegeven is ruim: het betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat ofwel naar een persoon herleidbaar is, bijvoorbeeld door middel van NAW, BSN of het IP-adres. Ook is het soms mogelijk om uit de context of met openbare gegevens te herleiden op wie de informatie betrekking heeft. Ook dan is er sprake van persoonsgegevens. Persoonsgegevens zijn opgedeeld in gewone persoonsgegevens, gevoelige persoonsgegevens en bijzondere persoonsgegevens. Ook hanteert UWV een eigen classificatie van persoonsgegevens.

Ook gepseudonimiseerde gegevens vallen onder het begrip persoonsgegevens. Volledig anonieme gegevens vallen niet onder de AVG. Wanneer het gaat om geanonimiseerde gegevens, moet advies ingewonnen worden bij JZ. Let op: Gegevens van overleden personen zijn geen persoonsgegevens in de zin van de AVG.

Voorbeelden
Een voorbeeld van een datalek met gewone persoonsgegevens is een brief met NAW-gegevens en algemene informatie over WW. Een voorbeeld van een datalek met gevoelige gegevens is een brief met BSN en financiële gegevens of een lijst met IP-adressen en surfgedrag op onze website. Een voorbeeld van een datalek met bijzondere persoonsgegevens is een brief met NAW en informatie over de gezondheid van een klant. Voorbeelden waarbij geen sprake is van persoonsgegevens: adresgegevens van bedrijven, algemene zakelijke e-mailadressen zoals info@bedrijf.nl (let op: zakelijke e-mailadressen met namen zijn wel persoonsgegevens, zoals jan.jansen@bedrijf.nl).

1.3. Is er sprake van een inbreuk in verband met persoonsgegevens (= datalek)?

Er is sprake van een datalek indien er sprake is van (1) een inbreuk op de beveiliging die (2) per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Toelichting
Allereerst moet vastgesteld worden of er sprake is van een beveiligingsincident. Er is dus niet uitsluitend sprake van een dreiging of een zwakke beveiliging (zowel technisch als organisatorisch), maar het beveiligingsincident heeft zich daadwerkelijk voorgedaan en dit heeft gevolgen voor verwerkte persoonsgegevens van betrokkene(n). Een voorbeeld: Een verkeerd adres dat niet conform ons proces in een systeem is opgenomen is een dreiging. Indien naar dit verkeerde adres een brief met persoonsgegevens wordt verstuurd, leidt deze dreiging tot een beveiligingsincident. Als de brief vervolgens geopend retour komt, is er sprake van een inbreuk in verband met persoonsgegevens. Als een adres van een klant wel conform ons proces in een systeem is gewijzigd kan er geen sprake zijn van een beveiligingsincident.

Ten tweede moet het beveiligingsincident er toe geleid hebben dat de persoonsgegevens (mogelijk) door een onbevoegde zijn ingezien, de persoonsgegevens zijn gewijzigd of de persoonsgegevens zijn vernietigd of (tijdelijk) niet beschikbaar geweest. Om het vorige voorbeeld door te trekken: als de brief ongeopend retour komt is er geen sprake van een inbreuk.

Er zijn dus drie categorieën datalekken te onderscheiden (ook wel de *aard* van het datalek):

1. *Inbreuk op de vertrouwelijkheid*
   Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens. *Let op: het mondeling doorgeven van persoonsgegevens is formeel geen verwerking. In het huidige meldformulier van de AP wordt geen toelichting gegeven of het mondeling doorgeven van persoonsgegevens aan een onbevoegde ontvanger als datalek bestempeld wordt. Wij zullen vooralsnog dergelijke incidenten behandelen volgens onze datalekprocedure.*

2. *Inbreuk op de integriteit*
   Wanneer er sprake is van onbevoegde of onopzettelijke wijziging van persoonsgegevens.

3. *Inbreuk op de beschikbaarheid*
   Wanneer er sprake is van een onbevoegd of onopzettelijk (tijdelijk) verlies van toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen. Het is belangrijk om te realiseren dat elke categorie zijn eigen risico's met zich meebrengt voor de rechten en vrijheden van de betrokkene.

Voorbeelden
Enkele voorbeelden van beveiligingsincidenten:

a) Persoonsgegevens die naar het verkeerde adres verzonden zijn.
b) Berichten met persoonsgegevens in de verkeerde Werkmap geplaatst.
c) Persoonsgegevens uit de systemen van UWV kunnen door een hack of een systeemfout gewijzigd dan wel vernietigd worden.
d) Een kwijtgeraakte laptop of USB-stick.
e) Klantgegeven tijdelijk niet beschikbaar door een ICT storing of fout.

Wanneer leiden bovenstaande beveiligingsincidenten tot een datalek?:

a) Er is sprake van een datalek als een poststuk geopend retour komt of de verkeerde ontvanger meldt dat hij of zij een verkeerd poststuk heeft ontvangen en opengemaakt. Als er een poststuk gesloten retour komt is er geen sprake van een datalek.
b) Er is sprake van een datalek als de onbevoegde klant daadwerkelijk de persoonsgegevens heeft ingezien.
c) Er is sprake van een datalek als de persoonsgegevens niet meer door een back-up terug gezet kunnen worden. Let op: ook als dit wel mogelijk is, kan nog steeds sprake zijn van een datalek doordat de persoonsgegevens niet beschikbaar zijn geweest.
d) Er is sprake van een datalek indien de laptop of USB niet op afstand kunnen worden gewist. Ook als dit wel mogelijk, kan nog steeds sprake zijn van een datalek, tenzij vastgesteld kan worden dat de persoonsgegevens op de laptop of USB niet geraadpleegd zijn.
e) Er is sprake van een datalek als door de (tijdelijke) onbeschikbaarheid de normale bedrijfsvoering van UWV is verstoord. Let wel, regulier onderhoud is geen datalek.

Let op: een foutieve adressering is niet verwijtbaar aan UWV als de klant aantoonbaar heeft nagelaten (tijdig) een postadres door te geven. Er is dan geen sprake van een beveiligingsincident. Ondanks dat de beoordeling dan stopt, kan het belangrijk zijn om de betrokkene wel op de hoogte te stellen en het poststuk alsnog juist toe te sturen.

ONDERDEEL 2: Risicobeoordeling

Dit onderdeel bevat de risicobeoordeling van een datalek. Voor het beoordelen van de risico's is het van belang dat alle informatie over het datalek beschikbaar is. Bij het inschatten van het risico moet gekeken worden naar (1) de ernst van de mogelijke gevolgen van het datalek en (2) hoe waarschijnlijk het is dat de gevolgen zich voordoen. Daarbij moeten het risico voor de betrokkene objectief beoordeeld worden.

Onderstaande factoren helpen om deze objectieve beoordeling vorm te geven. De factoren kunnen één voor één langsgegaan worden. Het is belangrijk om deze factoren te toetsen aan de specifieke omstandigheden van het datalek. Ook is het belangrijk om dit te documenteren in het meldingsformulier. Indien JZ om advies gevraagd wordt, stuur dan het volledig ingevulde interne meldingsformulier mee.

2.1. Factor: De aard van de inbreuk

Is er sprake van een inbreuk op de vertrouwelijkheid, integriteit of beschikbaarheid? Kortom zijn er persoonsgegevens gelekt, gewijzigd, niet beschikbaar of gewist? Elke aard neemt andere risico's met zich mee. Het verstrekken van medische gegevens aan een onbevoegd persoon heeft bijvoorbeeld andere gevolgen dan wanneer de medische gegevens zijn gewist.

2.2. Factor: De gevoeligheid en omvang van de persoonsgegevens

Dit is misschien wel een van de belangrijkste factoren. Hoe gevoeliger de gegevens, hoe groter het risico op schade. Ook indien de omvang van de gegevens groot is, zijn de risico's hoger.

2.3. Factor: Gemak waarmee betrokkenen kunnen worden geïdentificeerd

Deze factor heeft te maken met de herleidbaarheid. Als er een naam, adres of telefoonnummer betrokken is bij het datalek kunnen we er vanuit gaan dat de betrokkene makkelijk te identificeren is. Als gegevens gepseudonimiseerd zijn is het zeer moeilijk om de betrokkene(n) te identificeren, waardoor het risico sterk afneemt. Bij een inbreuk op de vertrouwelijkheid kan het verschil maken of de betrokkene en verkeerde ontvanger elkaar wel of geheel niet kennen. Kijk goed naar de omstandigheden of dit ertoe leidt of het risico daardoor groter wordt.

2.4. Factor: Ernst van de gevolgen (schade) voor personen

De gevolgen van een datalek kunnen ernstig zijn. Zo kan er sprake zijn van fysieke schade, bijvoorbeeld als iemand door het incident (tijdelijk) niet de benodigde zorg van de UWV bedrijfsarts krijgt. Ook kan sprake zijn van materiële schade, bijvoorbeeld wanneer iemand geen uitkering ontvangt en daardoor (extra) schulden maakt. Tot slot kan er sprake zijn van immateriële schade, bijvoorbeeld de angst van de *kans* op discriminatie of reputatieschade zonder dat dit zich daadwerkelijk heeft voorgedaan. Steeds vaker stellen betrokkenen UWV (terecht) aansprakelijk voor de schade. Goede documentatie is daarom van groot belang.

Let op: Als gegevens, waarop het medisch beroepsgeheim van toepassing is, terecht komen bij een onbevoegde, zijn er mogelijk ook tuchtrechtelijke gevolgen voor de arts.

2.5. Factor: Bijzondere kenmerken van de betrokkene

Wanneer gegevens van kwetsbare personen betrokken zijn bij het datalek, kunnen zij een groter risico op schade lopen. Zo kunnen er omstandigheden voordoen die het risico voor de betrokkene of personen nog groter maken, bijvoorbeeld als de betrokkene een geestelijke of lichamelijke

handicap heeft. Zo zal een klant die een Wajong-uitkering ontvangt in de regel kwetsbaarder zijn dan een klant met een WW-uitkering.

2.6. Factor: Bijzondere kenmerken van de ontvanger(s) (bij vertrouwelijkheid)

Het risico op ernstige gevolgen wordt kleiner wanneer de gegevens in handen zijn gekomen van een betrouwbare ontvanger. Voorbeelden van betrouwbare ontvangers zijn: partijen met wie UWV een vaste zakelijke relatie heeft, zoals een vaste samenwerkingspartner, en partijen die een wettelijk of professioneel beroepsgeheim hebben, zoals een huisarts, andere zorgverlener of advocaat (zie bijlage 2 voor een overzicht met potentiële betrouwbare ontvangers). Daarbij moet het aannemelijk zijn dat de onjuiste ontvanger geen kwaad in de zin heeft, bijvoorbeeld omdat hij zich houdt aan onze instructies (zie onderdeel 3).

Daarnaast kunnen de risico's lager zijn als er maar één of enkele verkeerde ontvangers zijn. Als de persoonsgegevens naar een grote groep mensen zijn gelekt kunnen de risico's een stuk groter zijn. Als de persoonsgegevens in de openbaarheid zijn geraakt, dan is er sprake van een zeer hoog risico. Dit omdat de gegevens voor eenieder toegankelijk zijn geweest. Ook als de onbevoegde ontvanger een medewerker van UWV is het risico lager, tenzij de betrokkene ook een medewerker van UWV is of als er opzet in het spel is.

2.7. Factor: Bijzondere kenmerken van onze organisatie

UWV is enerzijds een zelfstandig bestuursorgaan met taken op het gebied van werkloosheid, participatie en arbeidsongeschiktheid en anderzijds een werkgever. Toets altijd in welke hoedanigheid UWV optreedt. Gaat het bijvoorbeeld om een datalek met gegevens van een klant, gegevens van een medewerker van UWV, gegevens van een zakelijke klant of gegevens van een medewerker van een samenwerkingspartner?

2.8. Factor: Het aantal getroffen personen

Deze factor speelt geen rol bij de beoordeling van de meldplichtigheid. De gevolgen moeten altijd per individu beoordeeld worden. Een datalek met één betrokkene kan al ernstige gevolgen voor die persoon met zich meebrengen. Wel kan deze factor een rol spelen bij de kans dat de nadelige gevolgen daadwerkelijk intreden. Zo zal een groot Excel bestand met namen, e-mailadressen en telefoonnummers van een grote groep mensen veel interessanter zijn voor een cybercrimineel dan een brief met deze gegevens van slechts één persoon. Ook voor iemand die gestolen of onrechtmatig verkregen persoonsgegevens op het dark web wil verkopen, is een overzicht met persoonsgegevens van een grote groep mensen interessanter.

2.9. Factor: Effectieve maatregelen genomen

Indien sprake is van een inbreuk op de vertrouwelijkheid en er is slechts sprake van enkele onbevoegde ontvangers, dan kan contact met deze onbevoegde ontvangers ertoe leiden dat de risico's afnemen. Als deze onbevoegde ontvangers zich houden aan instructies, bijvoorbeeld door een poststuk terug te sturen of te bevestigen dat deze vernietigd is, kan dit het risico verlagen.

Het trekken van een conclusie

Het is belangrijk dat bovenstaande factoren worden toegepast op de specifieke omstandigheden van het geval. Geen datalek is hetzelfde. Kleine nuances kunnen er soms toe leiden dat de risico's veel groter of juist een stuk kleiner zijn.

Na het toepassen van de factoren op het datalek, is het van belang dat de specifieke factoren 'gewogen' worden en er een conclusie getrokken wordt. De ernst van de mogelijke gevolgen voor de betrokkenen dient te worden vermenigvuldigd met de kans daarop. De uitkomst kan worden ingedeeld in (1) verwaarloosbaar, (2) beperkt, (3) aanzienlijk en (4) zeer groot. Indien er sprake is van een zeer groot incident (en soms ook bij aanzienlijke incidenten, bij twijfel raadpleeg een Adviseur BG) dient het Calamiteitenplan Datalekken gestart worden, waarbij ook de FG geïnformeerd wordt.

Het is belangrijk om deze conclusie te onderbouwen en te documenteren, waarbij tevens gedocumenteerd kan worden of het datalek aan de AP gemeld zal worden (zie **onderdeel 3**) en/of betrokkene geïnformeerd wordt (zie **onderdeel 4**).

ONDERDEEL 3: Melden aan de AP

Na het afronden van de risicobeoordeling moet aan de hand van de uitkomst daarvan beoordeeld worden of het datalek gemeld dient te worden aan de AP. Indien meldplichtig, moet binnen 72 uur gemeld worden bij de AP. De termijn start zodra BG de interne melding heeft ontvangen en heeft vastgesteld dat de melding een datalek betreft. Het uitgangspunt is dat datalekken aan de AP gemeld worden, tenzij het niet waarschijnlijk is dat een risico voor de betrokkene of andere personen zal ontstaan. Dit laatste kan voorkomen als een van onderstaande situaties op het incident van toepassing is.

3.1. De ontvanger is betrouwbaar

Dit is het geval als (1) de onbevoegde ontvanger een wettelijke of professionele geheimhoudingsplicht heeft, zoals een advocaat, arts of overheidsmedewerker, en (2) deze ontvanger onze instructies opvolgt, zoals een toezegging om de ontvangen informatie te vernietigen dan wel te retourneren. Contact met de ontvanger is dus noodzakelijk. Indien de betrouwbare ontvanger een overheidsorganisatie is en de brief (automatisch) terug is gestuurd naar UWV, dan is contact niet noodzakelijk. Dit geldt ook als alleen 5.1 lid 2 sub e het poststuk heeft geopend. Zie bijlage 2 voor een overzicht van potentiële betrouwbare ontvangers.

3.2. Intern datalek

Als de onbevoegde ontvanger een medewerker van UWV is dan hoeft meestal ook niet gemeld te worden, een zogenaamde intern datalek. Dit komt omdat er voor UWV'ers een geheimhoudingsverplichting geldt: zij dienen zorgvuldig om te gaan met persoonsgegevens.

Let op: Dit kan anders liggen als er sprake is van een ernstig of groot intern datalek, bijvoorbeeld als er gegevens naar veel onbevoegde medewerkers zijn verstuurd of gevoelige gegevens van heel veel mensen naar een onbevoegde medewerker zijn verstuurd. Ook als een onbevoegde medewerker moedwillig, buiten zijn of haar taak, toegang heeft genomen tot de persoonsgegevens kan dit leiden tot een meldingswaardig incident. Tot slot ligt dit ook anders als de medewerker van UWV onbevoegd gegevens heeft ingezien van een (directe of oud-) collega. Ga dan na aan de hand van de omstandigheden en het contact met de betrokken medewerkers wat de kans is dat dit nadelige gevolgen heeft voor de medewerker in kwestie. Indien sprake is van opzet, verwijs de betrokken divisie dan ook naar Bureau Integriteit.

Een voorbeeld van een intern datalek is de situatie waarin er een arbeidsovereenkomst van een andere medewerker in Peoplesoft wordt gearchiveerd en een medewerker hier onbevoegd toegang tot krijgt. Er is sprake van een datalek en deze zal in de regel gemeld moeten worden, afhankelijk van de omstandigheden zullen betrokkenen ook geïnformeerd moeten worden. In dit soort situaties is het van belang om te kijken naar de omstandigheden van het geval, kennen de medewerkers elkaar? Zijn er andere risico's? Indien de situatie daartoe aanleiding kan geven kan er ook worden gekozen de betrokken manager de medewerker over het datalek te laten informeren.

Een ander voorbeeld van een intern datalek is de situatie waarin een medewerker een e-mail waarin informatie staat over UWV medewerkers, bijvoorbeeld of de arbeidsovereenkomst al dan niet wordt verlengd, verstuurt binnen UWV naar een ander onbevoegd algemeen e-mailadres. In deze situatie is er sprake van een datalek dat in de regel gemeld zal moeten worden. Omdat het hier gaat om een algemene mailbox zal er goed gekeken moeten worden naar de risico's. Wie heeft er toegang tot deze algemene mailbox en wie heeft deze e-mail gelezen? Is de e-mail daadwerkelijk verwijderd? Afhankelijk van de situatie zullen betrokkene(n) ook geïnformeerd moeten worden.

3.3. Verwaarloosbaar en kleinschalig datalek

Als het risico van het datalek vanwege de omstandigheden te verwaarlozen is. Dit is het geval als er een (zeer) beperkte set persoonsgegevens naar een verkeerde ontvanger is gestuurd. Bijvoorbeeld als een brief met een uitnodiging voor een banenmarkt, met alleen NAW-gegevens, bij een andere klant komt en er geen andere omstandigheden zijn die het risico verhogen. Een ander voorbeeld is een informatieve e-mail waarbij een beperkt aantal zakelijke e-mailadressen (met voor en/of achternaam) in het "Aan" veld zijn gezet in plaats van in de "BCC".

3.4. Adequate maatregelen vooraf

Als de gelekte gegevens doordat deze versleuteld waren door de onbevoegde ontvanger niet te herleiden zijn tot een persoon, dan is de kans dat er gevolgen optreden zeer klein.

Het is belangrijk dat als er gemeld wordt bij de AP, het meldingsformulier nauwkeurig wordt ingevuld, in overeenstemming met de informatie uit de overige documentatie. Bijlage 3 geeft richtsnoeren voor het invullen van het meldingsformulier. Indien binnen 72 uur alle informatie bekend is, dan wordt gelijk een definitieve melding gedaan. Als blijkt dat meer onderzoek vereist is en de beoordeling niet binnen 72 uur kan plaatsvinden, dan wordt een voorlopige melding ingediend. Tot slot, bij twijfel kan advies ingewonnen worden bij JZ.

ONDERDEEL 4: Informeren van betrokkene(n)

UWV moet het datalek melden aan betrokkene als zich waarschijnlijk een hoog risico kan voordoen voor de rechten en vrijheden van de betrokkene. De betrokkene moet "onverwijld" geïnformeerd worden. Hiervoor geldt geen wettelijke termijn. In de regel kan de betrokkene pas adequaat en volledig geïnformeerd worden nadat het onderzoek naar het datalek is afgerond en alle informatie bekend is. Het uitgangspunt is dat UWV betrokkene per brief informeert. Afhankelijk van de omstandigheden, bijvoorbeeld wanneer een klachtadviseur betrokken is, kan voor een andere communicatiemiddel gekozen worden. Het is wel noodzakelijk dat er een notitie over de inhoud van de melding aan betrokkene wordt opgesteld. Als het datalek niet aan de AP gemeld wordt, dan wordt de betrokkene ook niet geïnformeerd. Is het datalek gemeld aan de AP, dan moet beoordeeld worden of er sprake is van een hoog risico voor de betrokkene. De drempel om te melden aan de betrokkene ligt dus hoger dan de drempel om te melden aan de AP. Er zijn een aantal gevallen waarbij de betrokkene niet geïnformeerd hoeft te worden en er dus geen sprake is van een hoog risico.

Dit kan aan de orde zijn in de volgende situaties.

4.1. Beperkt en kleinschalig datalek

Als het gaat om een klein aantal persoonsgegevens die niet van gevoelige of bijzondere aard zijn. Een voorbeeld is een brief met NAW-gegevens en beperkte informatie over een WW-uitkering van de klant, waarbij geen sprake is van gezondheidsgegevens.

4.2. Adequate maatregelen achteraf

Achteraf zijn maatregelen genomen waarmee de vastgestelde risico's voor betrokkenen zijn weggenomen. Dit komt in de UWV-praktijk niet vaak voor.

4.3. Mededeling aan betrokkene onevenredig veel inspanning

De mededeling aan betrokkene onevenredig veel inspanning zou kosten. Dit komt niet snel voor, zeker omdat de betrokkenen ook via een openbare mededeling geïnformeerd kunnen worden. Dit geldt ook als het voor UWV niet mogelijk is om de betrokkene te informeren, bijvoorbeeld omdat er geen adres bekend is en de betrokkene in het BRP staat als "Vertrokken onbekend waarheen" (VOW-status).

4.4. Er is een zwaarwegend belang om niet te informeren

De betrokkene hoeft niet geïnformeerd te worden als dat noodzakelijk en evenredig is om een zwaarwegend belang te waarborgen. Zoals de nationale of openbare veiligheid of de bescherming van de privacy van anderen. Bijvoorbeeld wanneer door mededeling van het datalek bekend wordt dat iemand uit het gezin een melding heeft gedaan over de betrokkene.

De AP neemt als uitgangspunt dat in geval van twijfel de verwerkingsverantwoordelijke het zekere voor het onzekere dient te nemen en het datalek moet melden.

Let op: uitgangspunt is dat indien sprake is van een hoog risico betrokkene altijd geïnformeerd wordt, ongeacht de tijd die verstrekken is tussen het ontstaan van het datalek en de ontdekking daarvan. Hier kan vanaf geweken worden indien de omstandigheden van het geval daartoe aanleiding geven.

ONDERDEEL 5: Documentatieplicht

De AVG verplicht dat de verwerkingsverantwoordelijke alle datalekken documenteert, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Het is daarom van belang dat er een gestructureerd dossier wordt opgesteld van elk datalek en dat deze in het datalekregister komt. De AP kan UWV verzoeken om inzage te geven in het datalekregister. Ook komt het voor dat de betrokkene een schadeclaim indient; een overzichtelijk en volledig dossier is van groot belang voor een goede behandeling van een schadeclaim.

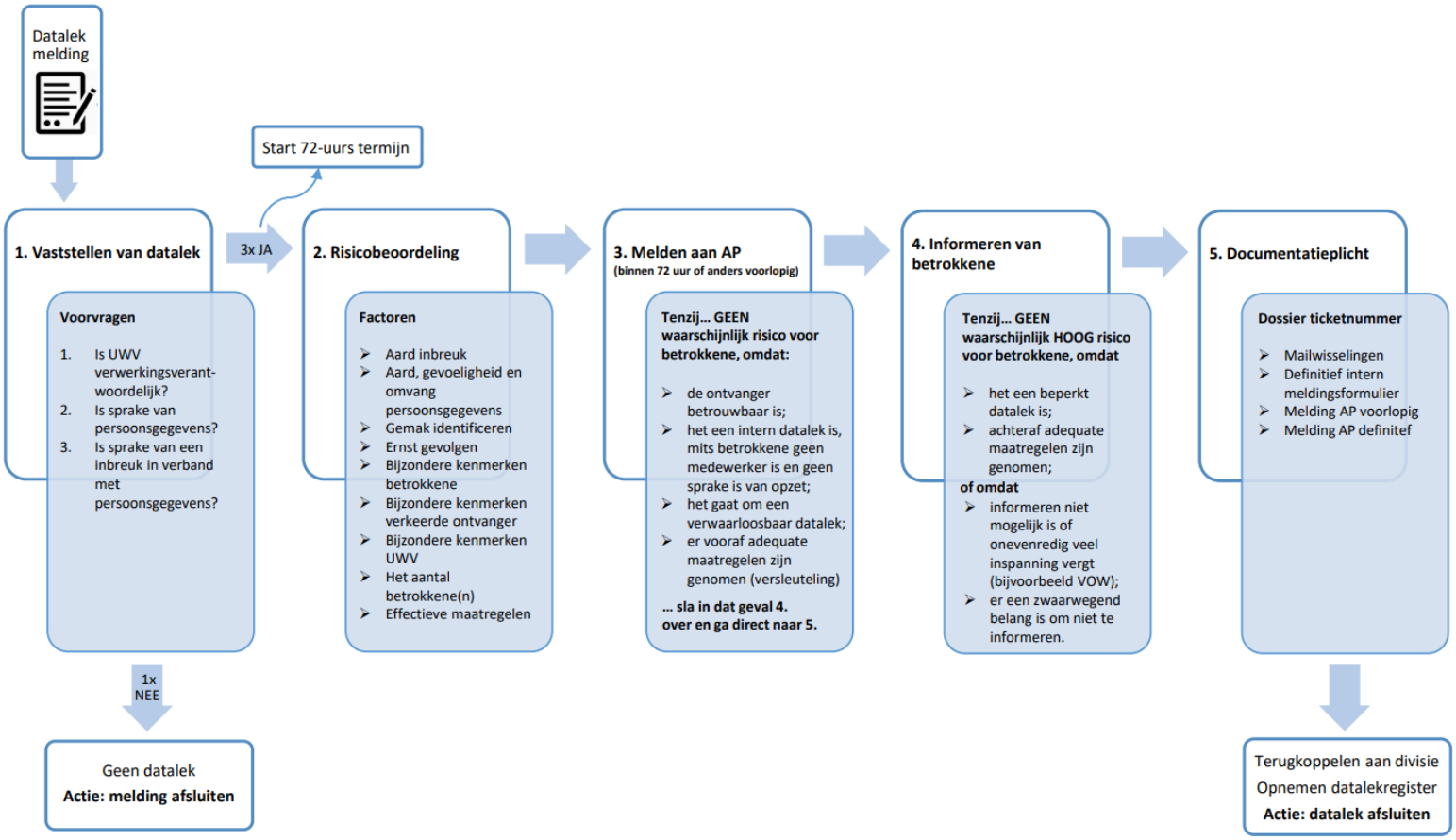
Als een divisie is aangesloten op Omnitracker dan wordt het dossier daarin opgebouwd. Voor de divisies die nog niet zijn aangesloten op Omnitracker, wordt het dossier nog opgebouwd in de digitale kluis. Een dossier bestaat in ieder geval uit de volgende documenten:

- Relevante mailwisselingen
- Indien van toepassing advies van JZ
- Definitief en volledig ingevuld intern meldingsformulier van het datalek
- Indien van toepassing de ontvangstbevestiging van de voorlopige en/of definitieve melding AP
- Indien van toepassing definitieve/getekende vaststellingsbrief zoals verstuurd aan de betrokkene(n)

Datum
9 december 2021

Versie
2.0

Bijlage 1: Stroomschema



Datum
9 december 2021

Versie
2.0

Bijlage 2: Vuistregels, betrouwbare ontvangers en praktijkvoorbeelden

Vuistregels

We kunnen de volgende vuistregels hanteren bij het trekken van een conclusie over de ernst van en de kans op mogelijke gevolgen. In onderstaande situaties gaat het telkens om het inzien van persoonsgegevens door een onbevoegde ontvanger. Deze vuistregels zijn richtinggevend, maar de specifieke omstandigheden van het geval kunnen altijd tot een andere conclusie leiden.

Verwaarloosbaar en kleinschalig (vaak niet meldplichtig, tenzij er twijfel is):

- Het gaat om niet gevoelige persoonsgegevens van één klant die door de onbevoegde ontvanger niet eenvoudig herleid kunnen worden naar de klant, bijvoorbeeld vanwege een verkeerd gespelde naam.
- Het gaat om een beperkte hoeveelheid persoonsgegevens van niet-gevoelige aard, zoals adresgegevens en algemene UWV klantinformatie, de onbevoegde ontvanger volgt onze instructies op of heeft de brief geretourneerd naar UWV.
- Het gaat om gevoelige en/of bijzondere persoonsgegevens van één of een beperkte groep klanten die intern naar een verkeerde medewerker van UWV zijn gestuurd, mits de gegevens niet van een andere medewerker zijn en de onbevoegde medewerker te goeder trouw is.
- Het gaat om gevoelige en/of bijzondere persoonsgegevens van één of een klein aantal klanten, maar de onbevoegde ontvanger is een betrouwbare ontvanger en er zijn geen andere factoren die het risico verhogen.

Beperkt (vaak meldplichtig, meestal ook betrokkene informeren):

- Het gaat om een beperkte hoeveelheid gevoelige persoonsgegevens, zoals financiële gegevens of het BSN, of een beperkte hoeveelheid gezondheidsgegevens, zoals enkel het recht op een bepaalde uitkering (WIA, WAZO, WAJONG) of een bepaalde ziekteperiode, van één of een klein aantal klanten en de onbevoegde ontvanger volgt onze instructies op.
- Het gaat om een grotere set niet-gevoelige persoonsgegevens van één klant, zoals een sollicitatiebrief met daarin NAW, historische werkgevers, genoten opleidingen en ambities.

Aanzienlijk (altijd meldplichtig, altijd betrokken informeren, soms calamiteitenplan datalekken opstarten):

- Het gaat om gevoelige persoonsgegevens, zoals financiële gegevens of BSN, van één of beperkte groep klanten en de onbevoegde ontvanger is niet te bereiken of volgt onze instructies niet op.
- De set persoonsgegevens betreffen uitgebreidere gezondheidsgegevens, medische gegevens of gegevens van strafrechtelijke aard van één of een kleine groep klanten. Er is sprake van gezondheidsgegevens als de informatie iets zegt over de gezondheid van de betrokkene.
- Het gaat om niet gevoelige persoonsgegevens van een grote groep klanten, bijvoorbeeld een Excel-bestand met NAW-gegevens en e-mailadressen van 100 of meer klanten van UWV.

Zeer groot (altijd meldplichtig, altijd betrokkene informeren, altijd calamiteitenplan datalekken opstarten):

- Deze inschatting van de ernst van de gevolgen is voor uitzonderlijke situaties bestemd en kan pas na zorgvuldige afweging gebruikt worden. Hiervoor moet (onder meer) een senior privacyjurist van de afdeling Juridische Zaken geraadpleegd worden.

Betrouwbare ontvangers en retour gekomen post

We kunnen onderstaande ontvangers in de regel als betrouwbaar classificeren. Let wel dat het belangrijk is dat er contact is geweest met de betrouwbare ontvanger. Indien de betrouwbare ontvanger een overheidsorganisatie is en de brief (automatisch) terug naar UWV is verstuurd, dan is contact niet noodzakelijk. Daarnaast is het van belang dat een betrouwbare ontvanger slechts één van de factoren is die meegewogen wordt. Let op: Het is dus niet per definitie zo dat als er sprake is van een betrouwbare ontvanger, de risico's daardoor te verwaarlozen zijn. Indien uit de overige omstandigheden alsnog blijkt dat er risico's zijn, dient het datalek, ondanks een betrouwbare ontvanger, bij de AP gemeld te worden en/of de betrokkene te worden geïnformeerd. Hier kan bijvoorbeeld sprake van zijn indien de betrouwbare ontvanger onze instructies niet opvolgt of indien er geen contact is geweest met de betrouwbare ontvanger.

Overzicht van onbevoegde ontvangers die betrouwbaar kunnen zijn:

- Andere overheidsorganisaties waarmee UWV een vaste relatie heeft, zoals:
  - Het ministerie van SZW
  - De SVB
  - De Belastingdienst
  - Gemeenten
  - Gemeenschappelijke regelingen (samenwerkingsorganisaties van gemeenten)
  - Europese overheidsinstellingen

- Partijen waarmee UWV een vaste zakelijke relatie heeft, zoals:
  - Vaste adviesbureaus
  - Vaste ICT leveranciers
  - Post

- Partijen die een wettelijk beroepsgeheim hebben, zoals:
  - (Huis)artsen
  - Medewerkers van ziekenhuizen
  - Zorgverleners
  - Professionele schuldhulpverleners
  - Bewindvoerders (ook nadat de bewindvoering is gestopt)
  - Advocaten
  - Medewerkers van een advocatenbureau
  - Notarissen
  - Gerechtsdeurwaarders

NB: Deze lijst kan aangevuld worden met nieuwe voorbeelden die voortvloeien uit de praktijk.

Richtlijnen bij niet retour gestuurde post

Indien een onbevoegde ontvanger melding maakt van een verkeerd ontvangen poststuk met persoonsgegevens of als op een andere manier blijkt dat een poststuk verkeerd is verzonden, hanteren we de volgende uitgangspunten voor het retour ontvangen van het poststuk.

Uitgangspunten
- In principe wordt altijd contact opgenomen met een melder/klant om te verzoeken de stukken retour te sturen om het risico van het incident zo veel mogelijk te beperken.
- Bij geen contact met bewoners van een adres wordt een brief gestuurd met het verzoek de stukken retour te sturen.

Hoe lang wachten we op retourpost?

- **2 weken** nadat klant/melder zegt de brief retour te hebben gestuurd wordt klant/melder nogmaals benaderd met de vraag of de stukken daadwerkelijk retour zijn gestuurd.
- Na dit gesprek nog **2 weken** wachten.
- Indien de post na **4 weken** totaal wachten nog niet retour is ontvangen, wordt het ticket gesloten met de melding dat het poststuk niet retour is gekomen.

Praktijkvoorbeelden

1. Kopie beslissing uitkering naar de verkeerde werkgever

Een belanghebbende werkgever dient een kopie beslissing uitkering van zijn werknemer te ontvangen. Dit betekent concreet dat de werkgever een begeleidende brief ontvangt, met daarbij een exacte kopie van de beslissing zoals de werknemer die heeft ontvangen. Dit gaat nog wel eens mis. Dit kan verschillende oorzaken hebben: zo kan een collega bij UWV het verkeerde aansluitnummer opvoeren en zo uitkomen bij een verkeerde werkgever of bij een klant/werknemer staat de verkeerde of een oude werkgever in het systeem. Deze brief wordt vaak door de werkgever geretourneerd.

- De persoonsgegevens zijn buiten UWV terecht gekomen: ze zijn onbevoegd verstrekt en onbevoegd ingezien. Deze fout is vaak aan UWV te wijten: ofwel een medewerker heeft een handmatige fout gemaakt, of er staat een fout in het ons systeem. Dit is afhankelijk van het specifieke geval.
- In deze brief bevinden zich persoonsgegevens, onder andere NAW, geslacht, BSN, financiële en soms gezondheidsgegevens van een werknemer die niet bij deze werkgever bekend is. Er zijn dus gevoelige persoonsgegevens bij het incident betrokken. In de brief is namelijk het recht op, de duur van en het hoogte van de uitkering opgenomen. Regelmatig staat hier ook een gezondheidsgegeven in, namelijk het soort uitkering. Een WIA, WAZO of WAJONG-uitkering zegt iets over je gezondheid.
- Het is niet onwaarschijnlijk dat de inbreuk een risico inhoudt voor de betrokkene: het is een meldplichtig incident. Hierbij wordt het volgende overwogen: het betreft een inbreuk op de vertrouwelijkheid van de gegevens en het gaat om een aanzienlijke set gevoelige en bijzondere persoonsgegevens. Deze persoon is makkelijk identificeerbaar: in de brief zijn het BSN en NAW-gegevens opgenomen. De mogelijke gevolgen kunnen ernstig zijn, omdat er gevoelige informatie van deze werknemer verkeerd terecht komen is. Daarbij is deze werknemer/klant afhankelijk van UWV voor het beschermen van zijn persoonsgegevens. Dit alles maakt dat de kans op risico's voor betrokkene niet onwaarschijnlijk is.
- Er is ook sprake van waarschijnlijk een hoog risico. Hierbij zijn doorslaggevend de aard van de gegevens (namelijk gevoelige en mogelijk bijzondere gegevens), de hoeveelheid persoonsgegevens, het feit dat de betrokkene makkelijk te identificeren is en dat de mogelijke gevolgen ernstig kunnen zijn.
- In het meldformulier van de AP wordt dit incident ingeschat met 'beperkt': ondanks de gevoeligheid van de gegevens is de post geretourneerd en de ontvangende partij betreft een zakelijke partij (werkgever).

2. Een WIA uitkeringsspecificatie wordt naar een verkeerd adres gestuurd

De klant ontvangt periodiek een WIA uitkeringsspecificatie per post. Doordat UWV een adreswijziging van de klant niet goed heeft doorgevoerd is de specificatie naar het oude adres verstuurd. Deze is geopend retour gekomen, waarna het datalekproces is gestart.

- De persoonsgegevens zijn door een onbevoegde ingezien. De fout is aan UWV te wijten.
- In de brief bevinden zich persoonsgegevens, namelijk NAW-gegevens, financiële gegevens en gegevens over de gezondheid (de uitkering voor WIA zegt namelijk iets over de gezondheid).
- Het is niet onwaarschijnlijk dat de inbreuk een risico inhoudt voor de betrokkene: het is een meldplichtig incident. Hierbij wordt het volgende overwogen: Het betreft een inbreuk in de vertrouwelijkheid van bijzondere persoonsgegevens. De betrokkene is makkelijk identificeerbaar en kwetsbaar. De mogelijke gevolgen zijn aanzienlijk. Zo kan een kwaadwillende UWV benaderen en proberen het rekeningnummer te laten wijzigen. Ook kan de klant benaderd worden over zijn of haar gezondheid.
- Er is ook sprake van een hoog risico. Naast het risico op financiële gevolgen, komt dit vooral omdat er gegevens over de gezondheid door een onbevoegde zijn ingezien.
- In het meldformulier van de AP wordt dit incident ingeschat met 'aanzienlijk'.

3. Een brief van Werkbedrijf met NAW-gegevens en BSN wordt verkeerd verstuurd

Een brief van Werkbedrijf wordt naar een verkeerde klant gestuurd omdat UWV een verkeerd adres heeft gebruikt. De brief bevat naast NAW-gegevens en werknemersgegevens geen gevoelige informatie, maar wel het BSN van de klant (deze is gebruikt als briefkenmerk). De verkeerde ontvanger heeft UWV gebeld en heeft de brief geopend retour gestuurd.

- De persoonsgegevens zijn door een onbevoegde ingezien. De fout is aan UWV te wijten.
- In de brief bevinden zich persoonsgegevens, namelijk NAW-gegevens, werknemersgegevens en het BSN.
- Het is niet onwaarschijnlijk dat de inbreuk een risico inhoudt voor de betrokkene: het is een meldplichtig incident. Hierbij wordt het volgende overwogen: Het betreft een inbreuk in de vertrouwelijkheid van persoonsgegevens. De betrokkene is makkelijk identificeerbaar. Ook is de klant mogelijk kwetsbaar. De mogelijke gevolgen zijn beperkt.
- Er is ook sprake van een hoog risico. Dit omdat het enkel gaat om een combinatie tussen NAW-gegevens en het BSN. De betrokkene wordt dus geïnformeerd.
- In het meldformulier van de AP wordt dit incident ingeschat met 'beperkt'.

4. Een VA of AD rapportage wordt handmatig aan de verkeerde envelop toegevoegd

Aan klanten worden verzekeringsgeneeskundige (VA) of arbeidsdeskundige (AD) rapportages verzonden. Dit vindt op dit moment plaats met een handmatig proces: collega's van UWV stoppen de juiste rapportage met de juiste begeleidende brief in een envelop. Soms komen twee rapportages in één envelop terecht, waardoor een rapportage bij de verkeerde klant terecht komt. Deze worden over het algemeen geretourneerd.

- De persoonsgegevens zijn buiten UWV terecht gekomen; ze zijn onbevoegd verstrekt en onbevoegd ingezien. De fout is aan UWV te wijten, nu een collega een handmatige fout heeft gemaakt in het werkproces. UWV is verwerkingsverantwoordelijke.
- In deze rapportages bevinden zich bijzondere persoonsgegevens, namelijk gezondheidsgegevens. Daarnaast zijn hierin onder meer naam, BSN en geboortedatum opgenomen. In de VA-rapportage kunnen zich medische gegeven bevinden. Er zijn dus persoonsgegevens bij het incident betrokken.
- Het is niet onwaarschijnlijk dat de inbreuk een risico inhoudt voor de betrokkene: het is een meldplichtig incident. Het gaat om een inbreuk op de vertrouwelijkheid van de gegevens en het betreft een aanzienlijke set bijzondere persoonsgegevens. De betrokkene is goed identificeerbaar en de mogelijke gevolgen kunnen ernstig zijn, omdat het om bijzondere persoonsgegevens gaat. De betrokkene heeft een afhankelijkheidsrelatie met UWV is en is voor de bescherming van zijn persoonsgegevens afhankelijk van UWV. De kans op risico's is daarmee niet onwaarschijnlijk.

- Dit incident zal, in overeenstemming met het voorgaande, gemeld moeten worden aan de betrokkene. Hierbij is doorslaggevend de aard en omvang van de set persoonsgegevens.
- In het meldformulier aan de AP wordt dit ingeschat met 'beperkt' voor de geretourneerde AD-rapportage en met 'aanzienlijk' voor de geretourneerde VA-rapportage.

5. Adresgegevens zijn verouderd in UPA, UZS of ODS. Daardoor wordt post naar het verouderde adres verzonden

Dit komt regelmatig voor en het is een bekend probleem. Wanneer een klant een adreswijziging aan UWV bekend maakt, worden verouderde correspondentie- of verblijfadressen niet automatisch aangepast in UPA, UZS en/of ODS.

Als de klant op de juiste wijze een adreswijziging aan UWV heeft doorgegeven aan UWV of aan de gemeente (BRP), maar UWV post stuurt naar een verouderd adres, dat in één van deze systemen is opgenomen, gaat het veelal om een meldplichtig incident. Er zijn altijd persoonsgegevens betrokken bij deze incidenten en de fout is aan UWV te wijten. Het incident moet (waarschijnlijk) gemeld worden aan de AP. Afhankelijk van de betrokken persoonsgegevens en andere relevante omstandigheden kan er sprake zijn van een hoog risico voor betrokkene. Dit is het geval als er in de brief gevoelige of bijzondere persoonsgegevens zijn opgenomen. In dat geval moet het incident gemeld worden aan betrokkene.

6. Bij het printen van dossiers worden verkeerd geplaatste stukken in EAED mee gestuurd

Deze fout doet zich vaker voor bij B&B. Deze divisie stuurt in het kader van bezwaar- en beroepsprocedures dossierstukken naar de betrokken klanten. Het komt voor dat in het elektronisch dossier van deze klant (in het systeem EAED) een document staat dat hier niet in thuis hoort. Het is dan onder het verkeerde BSN opgeslagen door DIV.

Het is vervelend wanneer dit gebeurt. Het is belangrijk dat de ontvanger de stukken van een andere klant aan UWV terug stuurt of vernietigd. In de meeste gevallen gaat het hier om een meldplichtig incident: er zijn persoonsgegevens bij betrokken en UWV heeft een fout gemaakt. Het is van belang dat de UWV-collega bij DIV een verzoek indient om dit document uit het verkeerde dossier in EAED te laten verwijderen. Het incident zal in de regel gemeld moeten worden aan de AP. Afhankelijk van de betrokken persoonsgegevens en andere relevante omstandigheden (het al dan niet retourneren, hoe makkelijk is de betrokkene te identificeren, welke mogelijke gevolgen zijn er voor betrokkene) kan er sprake zijn van een hoog risico voor betrokkene. In dat geval moet het incident gemeld worden aan betrokkene.

7. Klant heeft zelf geen adreswijziging doorgegeven, maar de post komt retour

In deze situatie moet vastgesteld worden dat UWV niet over het juiste adres van de klant beschikt en kon beschikken (er heeft dus geen controle met het BRP plaatsgevonden). Er zijn dan wel persoonsgegevens buiten UWV terecht gekomen (stap 1 en 2), maar dit is niet aan UWV te wijten. De klant draagt de verantwoordelijkheid om tijdig adreswijzigingen aan UWV of aan de gemeente door te geven. Deze incidenten meldt UWV niet aan de AP.

8. De werkgever stuurt post retour, maar hoort deze wel te krijgen

In deze situatie moet vastgesteld worden dat de werkgever belanghebbende is en de post in kwestie wel hoort te ontvangen. in dat geval is er geen sprake van beveiligingsincident. Er wordt daarom geen melding gedaan aan de AP of betrokkene: er zijn wel persoonsgegevens bij betrokken, maar er is geen sprake van een fout. De werkgever hoort deze post te ontvangen.

9. UWV heeft geen fouten gemaakt, maar de post wordt verkeerd bezorgd

In dit geval is UWV verwerkingsverantwoordelijke voor de postbezorging. Dit is gebaseerd op het standpunt van de AP. Nu 5.1 lid 2 sub e voor UWV de postbezorging verzorgt, is het mogelijk dat een postbezorger van 5.1 lid 2 sub e een fout maakt bij de bezorging. Dit betekent dat het om een meldplichtig incident gaat: er zijn persoonsgegevens bij betrokken, deze zijn buiten UWV op de verkeerde plek terecht gekomen. Het incident moet (waarschijnlijk) gemeld worden aan de AP. Afhankelijk van de betrokken persoonsgegevens en andere relevante omstandigheden kan er sprake zijn van een hoog risico voor betrokkene. In dat geval moet het incident gemeld worden aan betrokkene. Wanneer de betrokkene hiervan op de hoogte wordt gebracht, wordt een speciale vaststellingsbrief gebruikt specifiek gericht op onjuiste bezorging.

10. UWV heeft geen fout gemaakt, maar de post niet komt aan of post is kwijt

Het komt voor dat UWV post verstuurt aan het juiste adres van een klant, maar dat de klant laat weten dat de post niet is aangekomen. In dat geval is de post kwijt. Dit betreft vaak een meldplichtig incident. Hoewel het niet aan UWV te wijten is dat de post kwijt is, kunnen we niet uitsluiten dat er geen risico's zijn voor betrokkenen. Daarom gaat het vaak wel om een meldplichtig incident.

11. Verlies of diefstal van laptop/schijf/telefoon

Het komt voor dat een collega de zakelijke laptop, harde schijf of telefoon kwijt raakt of dat deze gestolen worden. De collega dient hiervan een melding te doen bij Bureau Integriteit (BI) en bij BG. Alle UWV hardware is encrypted: dit betekent dat ze op afstand 'gewiped' kunnen worden. Als de collega onverwijld melding heeft gedaan van het verlies van de hardware, kan ervoor gezorgd worden dat er geen sprake is van een datalek. De hardware wordt namelijk op afstand leeggehaald en er zijn dan geen persoonsgegevens meer betrokken bij het incident.

Let op: bij een dergelijk incident gelden aanvullende vragen die de IB&P teams aan de medewerker moeten stellen, het gaat om de volgende vragen:

1. *Kun je aangeven of je de Secure Mail contacten ooit gesynchroniseerd hebt met privé contacten?*
2. *Was er in de gestolen tas iets aanwezig waarin of waarop de pincode van de container (Secure Hub) vermeld stond?*
3. *Zijn UWV mails ooit doorgestuurd naar een privé emailadres van de medewerker (maakt niet uit of dit via laptop of telefoon is gedaan) en niet verwijderd, ook uit de prullenbak? Het gaat er om dat betreffende e-mails in het privédeel op een of andere wijze in te zien zouden kunnen zijn. Denk aan webmail via de browser op de smartphone of via een emailapp.*
4. *Indien het gaat om een laptop: Kun je aangeven of je wel eens werkgerelateerde informatie buiten de Citrix-omgeving (in Microsoft Teams, op het bureaublad of op de harde schijf) hebt opgeslagen? Zo ja, betreft dit persoonsgegevens van bijvoorbeeld klanten of collega's?*

12. Tijdelijke onbeschikbaarheid van persoonsgegevens door een systeemstoring

Het komt voor dat een systeem van UWV waarin persoonsgegevens worden verwerkt tijdelijk niet beschikbaar is. Indien zo'n incident bij de servicedesk wordt aangemeld als TOP incident (een incident met een hoge prioriteit) of als de servicedesk een risico ziet voor de persoonsgegevens, wordt er een vermoeden van een beveiligingsincident gemeld bij BG. Een beschikbaarheidsincident leidt tot een datalek als daardoor de normale bedrijfsvoering van UWV is verstoord.

Een voorbeeld van een beschikbaarheidsincident is wanneer een UWV klantportaal overdag voor 5 uur niet bereikbaar is door een storing. Klanten hebben daardoor hun persoonsgegevens niet kunnen inzien en ook geen persoonsgegevens kunnen aanleveren voor een aanvraag. Voor dit incident moet het datalekformulier ingevuld worden, gevolgd door een risicobeoordeling aan de hand van de criteria. Als de gevolgen voor klanten beperkt zijn en er maatregelen genomen worden, zoals verlenging van termijnen, zal een dergelijk incident in beginsel niet bij de AP gemeld hoeven worden. Als het klantportaal een hele dag of meerdere dagen onbeschikbaar is geweest, zal het incident waarschijnlijk wel gemeld moeten worden.

Een ander voorbeeld is wanneer het gehele WW-systeem op een werkdag 24 uur niet beschikbaar is door een storing. UWV-medewerkers hebben daardoor geen beoordeling kunnen maken op basis van persoonsgegevens. Ook hiervoor dient het datalekformulier ingevuld te worden gevolgd door risicobeoordeling. Gezien de aard en de omvang van de onbeschikbaarheid zal een dergelijk incident vaak wel gemeld moeten worden bij de AP, echter is dit ook sterk afhankelijk van de omstandigheden. Bij twijfel kan altijd JZ geraadpleegd worden.

13. Fout ergens in de keten waardoor UWV een datalek veroorzaakt

Een ander voorbeeld is de situatie waarbij er ergens in de keten een fout is gemaakt waardoor UWV een datalek veroorzaakt. Een voorbeeld hiervan is wanneer een overheidsinstelling incorrecte gegevens aanlevert, zoals een verkeerd postadres, waardoor UWV een datalek veroorzaakt. In dat soort situaties is er sprake van twee verwerkingen: de verstrekking van het verkeerde postadres van de overheidsinstelling aan UWV en het versturen van stukken aan het verkeerde postadres door UWV. De overheidsinstelling die de incorrecte gegevens heeft aangeleverd is niet verantwoordelijk voor de verstrekking van UWV aan het verkeerde postadres. UWV is zelf verwerkingsverantwoordelijke ten aanzien van het versturen van de stukken naar het verkeerde postadres. In deze situatie is er sprake van een datalek waar UWV verantwoordelijk voor is.

14. Een niet-dichtgeplakte envelop

Wanneer de klant een niet-dichtgeplakte envelop heeft ontvangen kan dit worden beschouwd als een beveiligingsincident, zolang het niet waarschijnlijk is dat zich een inbreuk heeft voorgedaan. Het is onwaarschijnlijk dat 5.1 lid 2 sub e de brief uit de envelop haalt. Indien de brief wordt bezorgd bij een huis met kamerverhuur waar maar één brievenbus is, is het aannemelijker om te spreken van een datalek. Wederom zijn de omstandigheden van het geval bepalend voor de beoordeling of er sprake is van een datalek of beveiligingsincident.

Bijlage 3: Meldformulier AP

Hieronder worden aantal richtsnoeren meegegeven voor het invullen van het meldformulier van de AP (in Google Chrome). Een aantal punten in het meldformulier spreken voor zich; deze zijn hieronder dan ook niet opgenomen. Zodra de AP een nieuw digitaal meldformulier beschikbaar stelt, zal deze bijlage aangepast worden.

2.1.
Onder 2.1 gaat het om de internationale aspecten. Deze komen bij datalekken bij UWV nagenoeg niet voor.

3.3.
Een organisatie is betrokken bij de inbreuk als deze een rol heeft gehad bij het ontstaan van de inbreuk. Het komt niet vaak voor dat een andere partij betrokken is bij het incident. Wel komt het voor dat een ketenpartner, zoals een gemeente, betrokken is bij het incident. De AP ziet UWV als verwerkingsverantwoordelijke voor postbezorging. 5.1 lid 2 sub e verzorgt de postbezorging voor UWV. Concreet betekent dit dat UWV verantwoordelijk is voor de postbezorging; ook als 5.1 lid 2 sub e of een andere postbezorger een fout maakt bij de bezorging.

4.
Wanneer het incident zich langere tijd heeft voorgedaan, of het onduidelijk is in welke periode deze precies heeft plaatsgevonden, moeten hier (bij benadering) een **startdatum** en een **einddatum** ingevuld worden. Dit is het geval als UWV een brief naar het verkeerde adres verzonden heeft. De startdatum is dan de dagtekening van de brief. De einddatum, namelijk de datum waarop UWV heeft vastgesteld dat het incident is gestopt, is de datum waarop UWV de brief retour heeft ontvangen.

Het incident doet zich nog voor als UWV het betreffende document nog niet retour heeft ontvangen, of het document nog in het verkeerde werkgeversportaal zichtbaar is. Het kan ook voorkomen dat de onjuiste ontvanger heeft aangegeven en bevestigd dat hij/zij de brief heeft vernietigd. Dit betekent ook dat het incident niet meer voordoet. Idealiter wordt dit zo snel mogelijk opgelost.

De inbreuk wordt vastgesteld en daarmee 'ontdekt' op het moment dat de medewerker het incident heeft beoordeeld en vaststelt dat er sprake is van een datalek. Dat is de datum van '**ontdekking'**.

Het uitgangspunt is om, na de vaststelling van de inbreuk, het datalek **binnen 72 uur** (voorlopig) te melden bij de AP. Indien het datalek geen hoog risico oplevert voor de betrokkene kan direct een **definitieve melding** worden gedaan. Indien de betrokkene wel geïnformeerd wordt is het raadzaam om binnen 72 uur de definitieve vaststellingsbrief te ontvangen en een definitieve melding te doen. Dit scheelt veel administratieve tijd. Alleen als er meer onderzoek nodig is of als het niet lukt om de vaststellingsbrief binnen 72 uur definitief te maken, kan een **voorlopige melding** worden gedaan.

5.
Bij UWV is bijna altijd sprake van **inbreuk op de vertrouwelijkheid** van de gegevens, persoonsgegevens zijn dan (mogelijk) ingezien door onbevoegden. Er kan ook sprake zijn van een **inbreuk op de integriteit** van de gegevens: de persoonsgegevens zelf zijn bijvoorbeeld gewijzigd (door bijvoorbeeld een hack). Ook komen **inbreuken op de beschikbaarheid** van de gegevens voor. Dit is bijvoorbeeld het geval als een UWV-systemen (tijdelijk) uitvalt, persoonsgegevens zijn dan tijdelijk of permanent niet beschikbaar.

5.3.
De samenvatting van het incident moet geschreven worden in de **eigen bewoording** van de medewerker. Probeer daarbij zoveel mogelijk gebruik te maken van de **terminologie** van de AP, zoals ook in het Toetsingskader is gebruikt.

6.
Toegangs- of identificatiegegevens zijn bijvoorbeeld inlognamen en wachtwoorden (zoals DigiD). **Locatiegegevens** betreffen bijvoorbeeld gegevens van Google Maps. Hiermee worden geen adresgegevens bedoeld. Onder het begrip **financiële gegevens** vallen ook gegevens over het recht op, de duur van en de hoogte van een uitkering. UWV verwerkt hoofdzakelijk gegevens over iemands **gezondheid**; dit invulveld wordt daarom vaak met 'ja' beantwoord. Het feit dat een klant een ziektewetuitkering ontvangt, is al een gezondheidsgegeven. Het gaat zelden om **genetische** of **biometrische** gegevens.

In het meldformulier wordt gevraagd om aan te geven hoeveel **gegevensrecords** (**gegevensregisters**) zijn getroffen door de inbreuk. Een gegevensrecord is een vastlegging van informatie over een bepaald persoon. Een gegevensrecord kan meerdere (categorieën van) persoonsgegevens bevatten.

Voorbeelden:
- Een brief is één gegevensrecord, eventuele bijlagen zijn aparte gegevensrecords
- Bij een lijst is vaak elke regel één gegevensrecord, bijvoorbeeld één regel in een Excelbestand.
- Een kopie paspoort is ook één gegevensrecord.
- Bij logging is elke logregel één gegevensrecord.

7.
Hier vult de medewerker in wie de betrokkenen bij de inbreuk zijn. Dit zijn bijna altijd **klanten (huidig en potentieel)**. In een enkel geval betreffen het werknemers, als persoonsgegevens van medewerkers bijvoorbeeld gelekt zijn. De groep mensen van wie de persoonsgegevens betrokken zijn bij het incident wordt omschreven als 'klanten van UWV' of 'medewerkers van UWV'. Personen uit kwetsbare groepen zijn vaak personen die zeer nadelige gevolgen kunnen ondervinden wanneer hun persoonsgegevens publiekelijk beschikbaar zouden worden. Indien er ook sprake is van een groep klanten (of medewerkers) die extra kwetsbaar zijn, zoals klanten met een Wajong-uitkering, kies dan ook 'Ja' bij '**Personen uit kwetsbare groepen**'. Bij de afweging of betrokkene aangemerkt kan worden als een persoon uit een kwetsbare groep moet altijd gekeken worden naar de omstandigheden van het geval.

8.
Er zijn vaak geen maatregelen getroffen zoals die onder 8 omschreven zijn. In een enkel geval is dit wel aan de orde.

9.1.
Onder 9.1 is het gebruikelijk om kenbaar te maken dat bij het specifieke incident **onbevoegden kennis hebben kunnen nemen van de gegevens** en dat deze op **een onbehoorlijke of onrechtmatige manier gebruikt kunnen worden**. Wanneer UWV bijvoorbeeld een oud adres van een klant in het systeem heeft staan en dit heeft gebruikt, moet ook het derde invulveld met 'ja' beantwoord worden. In dat geval worden namelijk intern onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt.
Het komt zelden voor dat de overige drie invulvelden met 'ja' moet worden beantwoord.

9.2.
Onder 9.2 gaat het om de mogelijke schade voor betrokkenen. Dit betreft een inschatting die afhankelijk is van het soort persoonsgegevens dat betrokken was bij het incident en de hoeveelheid persoonsgegevens. **Discriminatie** komt geregeld voor, maar dit is afhankelijk van de aard en inhoud van de persoonsgegevens. Er is vaak sprake van een kans op **identiteitsdiefstal of – fraude**. **Financiële verliezen** komen zelden voor. **Reputatieschade** komt vaak voor.

Wanneer persoonsgegevens, die onder het medisch beroepsgeheim vallen, bij het incident betrokken zijn, moet ook het invulveld bij **verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens** met 'ja' worden beantwoord.

Vervolgens vraagt de AP om een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen. Hier vindt altijd een belangenafweging plaats, waarbij goed gekeken wordt naar de omstandigheden van het specifieke geval. Deze zijn uitgewerkt in **de risicobeoordeling**. Bij de toelichting van de risicobeoordeling kan gebruikt worden gemaakt van onderstaande standaardzinnen.

Indien gekozen wordt voor **beperkt** risico:
- De melder heeft uit eigen beweging contact opgenomen met UWV en tevens onze instructies opgevolgd om de brief/stukken retour te sturen. Gelet op de persoonsgegevens die betrokken zijn bij de inbreuk en de medewerking van de onbevoegde ontvanger wordt de ernst van de mogelijke gevolgen voor de betrokkene op beperkt geschat.

Indien gekozen wordt voor **aanzienlijk** risico:
- Aangezien er persoonsgegevens bij de inbreuk betrokken zijn die normaliter beschermd worden door het medisch beroepsgeheim wordt de ernst van de mogelijke gevolgen voor de betrokkene op aanzienlijk geschat.
- Omdat UWV de brief/stukken niet in bezit heeft en UWV zodoende niet weet waar de brief/stukken zich bevinden kan UWV geen maatregelen nemen om de inbreuk tegen te gaan. Derhalve schatten wij de ernst van de mogelijke gevolgen op aanzienlijk.
- Gezien de grote hoeveelheid gegevensrecords (en de gevoeligheid van de persoonsgegevens) die betrokken zijn bij de inbreuk schatten wij de ernst van de mogelijke gevolgen voor de betrokkenen op aanzienlijk.

10.
Uit de beoordeling volgt of er een vaststellingsbrief naar de betrokkene verzonden wordt. Bij 10.1, de **inhoud van de melding aan betrokkenen** wordt de inhoud van de brief letterlijk opgenomen (geanonimiseerd). Het is belangrijk dat de divisie de inhoud van de vaststellingsbrief snel terugkoppelt, zodat de meldingen binnen 72 uur definitief kunnen worden ingediend. Het uitgangspunt is dat UWV een brief als **communicatiemiddel** gebruikt. Afhankelijk van de omstandigheden, bijvoorbeeld als een klachtadviseur betrokken is, kan voor een andere communicatiemiddel gekozen worden. Een notitie van de inhoud van de melding aan de betrokkene is dan wel noodzakelijk.

Wanneer afgezien wordt van de melding aan betrokkenen, moet dat hier verwoord worden. Dit volgt uit de conclusie dat er **geen sprake is van een hoog risico** voor de betrokkene (zie hiervoor de risicobeoordeling).

10.3.
Onder 10.3 worden de door UWV genomen maatregelen opgenomen, om herhaling van dit incident in de toekomst te voorkomen. Dit is afhankelijk van het soort inbreuk. Zo kan er een aanpassing gedaan worden in een handmatig proces, kan een systeemfout opgelost worden of wordt een verouderd adres uit onze adressystemen verwijderd. Probeer de verwoording van het interne meldformulier zoveel mogelijk aan te houden. Zorg dus ook dat de divisie duidelijk heeft aangegeven welke maatregelen zij getroffen hebben.

11.
Om een voorlopige melding te doen, wordt hier geselecteerd dat de melding nog niet compleet is en dat er een aanvullende melding zal volgen. Is de melding volledig ingevuld en afgerond? Dan kan de melding definitief gemaakt worden.

Indien er wordt gekozen voor een voorlopige melding moet er binnen vier weken een vervolgmelding worden gemaakt waarin er een update gegeven wordt aan de AP. Indien er geen vervolgmelding wordt gemaakt voldoet UWV niet aan de meldplicht op grond van artikel 33 AVG.

Let op: je ontvangt géén kopie van de melding. Je kunt het formulier wel downloaden direct nadat je het hebt verstuurd. Zorg ervoor dat je doorklikt naar de laatste pagina om dit te kunnen doen. Sla het formulier op als PDF in het dossiermapje met als naam "Melding AP voorlopig" of "Melding AP definitief". Op het meldingsformulier bevindt zich ook het unieke identificatienummer van de AP. Dit nummer gebruik je als je een voorlopige melding definitief wilt maken.