Ministerie van Onderwijs, Cultuur en Wetenschap

Concept Verwerkersovereenkomst beleidsgericht onderzoek onderwijs <Onderwerp/titel nadere overeenkomst,

ten behoeve van

de Staat der Nederlanden, het Ministerie van Onderwijs, Cultuur en Wetenschap

behorende bij de afgesloten raamovereenkomst Beleidsgericht Onderzoek Onderwijs (ROK BGOO 2026), perceel <vul perceelnummer + perceel naam in> vanuit EU- aanbesteding met kenmerk BD-EURAAN-RD-IUCN2502 (TN509789)

Status	Publicatieversie (7 april 2025)
Kenmerk Tender	<Vul het TN-nummer van de minicompetitie in>
Kenmerk minicompetitie	<Vul het IUCN-nummer in>

Toelichting t.b.v. de EU-aanbesteding
Zoals opgenomen in de aanbestedingsstukken sluit opdrachtgever per perceel een raamovereenkomst (ROK) met meerdere opdrachtnemers. Vervolgens worden opdrachten via minicompetities uitgezet onder de raamcontractanten. Met de winnaar van de minicompetitie wordt een nadere overeenkomst (NOK) gesloten.

Indien van toepassing op het onderwerp van onderzoek wordt als onderdeel van de NOK nog aanvullend een Verwerkersovereenkomst (VWOK) afgesloten. Bijgesloten document is de basis van iedere VWOK die wordt afgesloten.

Opdrachtgever (het Bestuursdepartement) dient per minicompetitie keuzes te maken ten aanzien van bepaalde standaardartikelen uit de VWOK. Deze keuzes zijn in deze conceptovereenkomst aangeven.

Legenda

Kleur gemarkeerde tekst	Toelichting
	Grijs gemarkeerde tekst bevat optionele artikelen. Opdrachtgever stelt per minicompetitie een op maat gemaakte concept NOK op. Afhankelijk van de aard van de opdracht wordt de grijze tekst geschrapt, of opgenomen in de concept NOK.
	Bij geel gemarkeerde tekst maakt Opdrachtgever een keuze uit twee alternatieve teksten. Afhankelijk van de aard van de opdracht wordt door Opdrachtgever een keuze gemaakt welke optie wordt opgenomen in de NOK.
	Groen gemarkeerde tekst bevatten velden die specifiek per NOK ingevuld worden. Inhoud van deze velden hebben meestal betrekking op een datum, kenmerken, (contact)personen, e.d.

Instructie:

- Voor zover teksten '<*OPTIONEEL*>' zijn is dat aangegeven in de tekst.
- Bij teksten waar 'OF' tussen de bepalingen in staat, dient een keuze tussen de verschillende opties gemaakt te worden. De overige optie(s) verwijderen uit de overeenkomst.
- Deze Verwerkersovereenkomst vormt een onlosmakelijk geheel met een op de ARVODI-2018 gebaseerde Overeenkomst en kan derhalve alleen in combinatie daarmee worden gesloten. Bepalingen over geheimhouding, aansprakelijkheid e.d. die in in de Overeenkomst zijn vastgelegd, hoeven derhalve niet nog eens afzonderlijk in de Verwerkersovereenkomst te worden opgenomen. Zie voor meer informatie de Toelichting bij het gebruik van het Model Verwerkersovereenkomst ARVODI (te vinden op Rijksportaal).

(Datum: februari 2024)

Concept VERWERKERSOVEREENKOMST

Met kenmerk (IUCN-nummer), […kenmerk NOK…], inzake [perceel] en referentienummer [verpl. nr.]

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag,
te dezen vertegenwoordigd door de Minister van Onderwijs, Cultuur en Wetenschap (OCW),
namens deze,
[Naam en functie ondertekenaar OCW (Bestuursdepartement)]
Hierna te noemen: Opdrachtgever

en

2. [Naam Opdrachtnemer(s)]
KvK nummer [KvK nummer Opdrachtnemer], statutair gevestigd te [Statutaire vestigingsplaats Opdrachtnemer]
te dezen vertegenwoordigd door
[Naam en functie ondertekenaar Opdrachtnemer] hierna te noemen: Opdrachtnemer,

Toelichting: indien een partij voor de ROK heeft ingeschreven als Samenwerkingsverband, dan wordt de nadere overeenkomst afgesloten met alle partijen in het Samenwerkingsverband. Als er sprake is van een Samenwerkingsverband dan nemen we alle deelnemers op als ondertekenaar van deze Raamovereenkomst. Ingeval van een Samenwerkingsverband is aangewezen penvoerder gemachtigd om nadere overeenkomsten te tekenen namens alle partijen.

Let op: voor alle deelnemers geldt **hoofdelijke aansprakelijkheid**, ook voor nadere overeenkomsten waarvoor de feitelijke uitvoering door slechts één of een deel van het Samenwerkingsverband wordt uitgevoerd.

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, kwalificeert Opdrachtgever als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als Verwerker;
- Partijen in deze Verwerkersovereenkomst (VWOK), zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.
- Deze Verwerkersovereenkomst (Contractbijlage 3) is onlosmakelijk verbonden met de bovenliggende Nadere overeenkomst (NOK) vanuit de raamovereenkomst Beleidsgericht onderzoek onderwijs (ROK BGOO 2026). De NOK bestaat naast onderhavige VWOK in bijlage 3 uit:
    - Contractbijlage 1: offerteaanvraag, nota van inlichtingen en alle overige relevante aanbestedingsdocumenten
    - Contractbijlage 2: de door Opdrachtnemer ingediende winnende offerte

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de ARVODI-2025 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst zijn toegespitst. Aldus en in aanvulling daarop wordt onder de volgende begrippen, ongeacht of ze in meervoud of enkelvoud, of als werkwoord of zelfstandig naamwoord worden gebruikt, in deze Verwerkersovereenkomst verstaan:

1.1 ARVODI-2025: Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2025.

1.2 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.3 EER: Europese Economische Ruimte, zijnde alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

1.4 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die 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 gegevens.

1.5 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de Persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk Persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als Ontvangers; de Verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.

1.6 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer [titel] van [datum], met kenmerk [kenmerk].

1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever Verwerkt.

1.8 Toezichthoudende autoriteit: een door een lidstaat ingevolge artikel 51 van de Verordening ingestelde onafhankelijke overheidsinstantie.

1.9 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.10 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.

1.11 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.12 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1.13 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking door Opdrachtnemer in het kader van de Overeenkomst en is onlosmakelijk verbonden met de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en Ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat Opdrachtnemer alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 10 van deze Verwerkersovereenkomst.

3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Opdrachtnemer van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Opdrachtnemer Opdrachtgever voorafgaand aan de Verwerking in kennis van dat wettelijk voorschrift, tenzij dat wettelijk voorschrift deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4.2 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

Artikel 5. Beveiliging van de Verwerking

5.1 Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, treft Opdrachtnemer aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of tekortschieten (in de naleving van) technische en organisatorische beveiligingsmaatregelen zoals bedoeld in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2025.

6.2 Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2025.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2025, een andere Verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere Verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Opdrachtnemer Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.

8.3 Opdrachtnemer stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan Opdrachtgever.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf te maken kosten gerelateerd aan de Inbreuk in verband met Persoonsgegevens.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Opdrachtnemer er zorg voor dat hij, naar gelang de keuze van Opdrachtgever, alle Persoonsgegevens wist of terugbezorgt aan Opdrachtgever en bestaande kopieën verwijdert, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.
<OPTIONEEL> In geval van wissen en/of verwijderen van kopieën door Opdrachtnemer informeert hij Opdrachtgever zodra hij dit heeft gedaan.

10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Opdrachtnemer zorg voor het wissen of terugbezorgen en het verwijderen van kopieën van de betreffende Persoonsgegevens, tenzij opslag van deze Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.

10.3 **<OPTIONEEL>** Opdrachtnemer [wist of bezorgt terug] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag]. Betaling van de boete laat de verplichtingen uit artikel 10 en de gehoudenheid van Opdrachtnemer om de schade die het gevolg is van de schending te vergoeden onverlet.

10.4 **<OPTIONEEL>** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.

OF

10.4 **<OPTIONEEL>** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze van terugbezorging inclusief vermelding beveiligingsmaatregelen] [adres].

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtgever kan een audit van de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten (laten) uitvoeren als concrete omstandigheden daartoe aanleiding geven. Opdrachtnemer verleent alle medewerking aan audits, waaronder begrepen audits bij Personeel van Opdrachtnemer, tenzij dit redelijkerwijs niet van hem kan worden verwacht.

11.3 Opdrachtnemer stelt Opdrachtgever onmiddellijk in kennis indien naar zijn mening een instructie van Opdrachtgever in het kader van artikel 11 eerste en/of tweede lid van deze Verwerkersovereenkomst, inbreuk oplevert met een wettelijk voorschrift inzake gegevensbescherming.

11.4 Partijen dragen zelf de kosten die zij maken in verband met de in dit artikel bedoelde informatieverstrekking en audits, waaronder begrepen de kosten van door hen ingeschakelde derden.

11.5 Opdrachtgever is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Opdrachtnemer is gehouden aan die maatregelen in redelijkheid uitvoering te geven.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

	Opdrachtgever:	**Opdrachtnemer / of Penvoerder namens het gehele samenwerkingsverband**
Plaats	Den Haag	…
Datum	…	…
Functie en naam ondertekenaar	De Minister van Onderwijs, Cultuur en Wetenschap namens deze, …	…
Handtekening		

Bijlage 1. De Verwerking van Persoonsgegevens

Instructie:

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

N.B. bij gebruik van de bijlage, deze instructietekst verwijderen.

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Overzicht Verwerkingen

Het onderwerp, aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
……	

<OPTIONEEL indien aan de orde**>**
Subverwerker(s)

Naam en contactgegevens subverwerker	
Nummer handelsregister van subverwerker	
Het onderwerp, aard en doel van de Verwerking	
Het soort Persoonsgegevens	
Beschrijving categorieën van Persoonsgegevens	
Beschrijving categorieën Betrokkenen	
Beschrijving categorieën Ontvangers van Persoonsgegevens	
Locatie Verwerking Persoonsgegevens	
……..	

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens (waaronder datalekken)

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Procedure Opdrachtgever
Zie bijgevoegd bij dit document: "Procedure Opdrachtgever: Melden, afhandelen en oplossen datalek".

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Datum en tijdstip van de constatering van de (vermoedelijke) Inbreuk in verband met Persoonsgegevens
Aard van de Inbreuk in verband met Persoonsgegevens
De soort, categorieën en het aantal Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Procedure Opdrachtgever: Melden, afhandelen en oplossen datalek

Ministerie van Onderwijs, Cultuur en Wetenschap

Melden, afhandelen en oplossen datalek

Documentdatum: 03-06-2021

Inhoudsopgave

1. Melden, afhandelen en oplossen datalek

Procesinformatie	
Proceseigenaar	directeur BOA
Procesbeheerder (naam en functie)	Maartje Breeman, adviseur Informatiebeveiliging & Privacy (AIP)
Materiedeskundige(n)	Ewald Nijenhuis (FG), Maartje Breeman
Opsteller procesbeschrijving	Safieka Imamkhan
Status	Definitief
Datum	04-06-2021
Evaluatiedatum	11-11-2021
Classificatie	Strategisch-kritisch
Relevante kaders	Artikel 33 AVG Artikel 34 AVG Uitvoeringswet Alg. verordening gegevensbescherming (AVG) Privacybeleid OCW Guidelines Datalekken vd European Data Protection Board (EDPB) Richtlijnen voor Functionarissen Gegevensbescherming Baseline Informatiebeveiliging Overheid (BIO) IB Incidentenbeleid OCW

Informatiebeveiliging	
AVG/PIA	Er is geen PIA nodig. De verwerking wordt wel opgenomen in het verwerkingsregister
ICT-systemen	Proza en Outlook
Autorisatie(s) toegekend	Register datalekken is alleen toegankelijk voor: AI&P en FG, CISO, BVA
Bewaar-/Vernietigingstermijn	5 jaar bewaren, daarna vernietiging persoonsgegevens (Generieke Selectielijst, 5.2), register zonder persoonsgegevens bewaren

Procesdoel
Dit proces kent meerdere doelen:
- Het op gecontroleerde wijze omgaan met de gevolgen van een datalek;
- Voldoen aan artikel 33 en 34 Algemene Verordening Gegevensbescherming (AVG), waaronder het tijdig melden van risicovolle meldingsplichtige datalekken bij de toezichthouder (Autoriteit Persoonsgegevens (AP)) en het bijhouden van een register met alle meldingen;
- Medewerkers weten waar, hoe en wanneer zij (een vermoeden van) een datalek moeten melden.

(Kritische) prestatie indicatoren
- Alle OCW medewerkers weten dat een (mogelijk) datalek intern gemeld moet worden bij Meldpuntdatalekken@minocw.nl en dat zij moeten verifiëren dat het datalek gedicht wordt.
- De directie meldt het datalek direct na ontdekking, maar hoogstens binnen een werkdag via het formulier aan het meldpunt datalekken via mailto:meldpuntdatalekken@minocw.nl
- De directie meldt meldingsplichtige datalekken binnen 72 uur bij de Autoriteit Persoonsgegevens.
- Er is een centraal datalekkenregister voor BD dat voldoet aan gestelde vereisten.

Scope/Bereik
Deze procesbeschrijving is van toepassing op het bestuursdepartement (BD).

Fatale termijnen
Datalekken moeten altijd intern gemeld en geregistreerd worden. Wanneer het risicovolle datalekken betreft, moeten deze binnen 72 uur gemeld worden aan de toezichthouder AP. Bij twijfel doet de gemandateerd verwerkingsverantwoordelijke (de desbetreffende directie) binnen die termijn een voorlopige melding. Deze kan op later moment (maar binnen twee á vier weken) aangevuld dan wel ingetrokken worden. Datalekken met een hoog risico moeten gemeld worden aan de betrokkene. Hier zijn geen termijnen aan verbonden.

Korte (proces)beschrijving
Het is een eerstelijns verantwoordelijkheid van de directie om te zorgen dat medewerkers een datalek kunnen herkennen, dat actie ondernomen wordt om het datalek te (laten) dichten en deze te melden (intern, maar mogelijk ook bij toezichthouder en betrokkenen). De directeur bepaalt welke functionaris welke rol vervult.

1. Ontdekken: Iemand ontdekt een (vermoedelijk) datalek en meldt dit bij diegene die verantwoordelijk is voor het proces waarbinnen het datalek plaatsvond. Deze licht de privacy contactpersoon (PC)[1] van de verantwoordelijke directie in;
2. Onderzoek en start registratie: de PC vergaart informatie over het incident en informeert de directeur;
3. Dichten datalek: de PC verifieert dat de acties ondernomen worden om het datalek te dichten. Stap 3 & 4 vinden gelijktijdig plaats;
4. (intern) Melden -binnen 24 uur- aan de FG via het MeldpuntDatalekken@minocw.nl, met een cc aan de eigen directeur. Doel:
   o Consultatie FG om gezamenlijk te bepalen wat de aard van het risico is t.b.v. het voldoen aan de meldplicht datalekken en;
   o Om als bestuursdepartement een centraal datalekregister aan te leggen en daarmee te voldoen aan de registerplicht;
5. Advisering directeur: de PC stelt een advies op voor de directeur:
   o Over de afhandeling van het datalek zelf en;
   o Over de ernst van het datalek;
   o Of het datalek moet worden gemeld aan de AP en zo ja, of het dan ook gemeld moet worden aan de betrokkene(n);
6. (extern) Melden Datalekken bij AP en intern informeren:
   o de directeur wijst een medewerker aan die het meldingsplichtige datalek meldt aan de Autoriteit Persoonsgegevens via het voorgeschreven meldingsformulier Autoriteit Persoonsgegevens. De CISO en de FG (via meldplichtdatalekken@minocw.nl) worden altijd geïnformeerd na melding bij de AP;
   o Zo nodig, afhankelijk van de ernst en gevoeligheid van het datalek, informeert de directeur de DG en SG.
   o De beveiligingsambtenaar (BVA) wordt geïnformeerd als het datalek ook gerubriceerde informatie, systemen of apparaten betreft.
7. (extern) Melden bij betrokkenen: bij datalekken met een hoog risico voor de betrokkenen, meldt de directeur het datalek ook aan de personen van wie persoonsgegevens betrokken waren in het datalek. Afstemming zoeken met directie Communicatie.
8. Afronding. De PC rondt e.a. administratief af en zendt de laatste versie van het formulier naar meldpuntdatalekken@minocw.nl. De FG neemt het definitieve formulier op in het Register van Datalekken (RD).

Achtergrondinformatie: Wat is een datalek?
Er is sprake van een datalek[2] bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens.

Er zijn 3 types datalekken te onderscheiden:
- Inbreuk op de vertrouwelijkheid

Onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- Inbreuk op de integriteit

Onbevoegde of onopzettelijke wijziging van persoonsgegevens.

[1] Er is een lijst contactpersonen bekend bij de FG & AIP. In Q2 2021 wordt bij alle directies uitgevraagd de contactpersonen te (her)bevestigen.
[2] De AVG spreekt niet van een datalek maar van een 'inbreuk in verband met persoonsgegevens'. Zie artikel 4, punt 12 van de AVG.

- Inbreuk op de beschikbaarheid

Onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Voorbeelden:
- Verlies of diefstal van een datadrager (telefoon, laptop, USB-stick, ordner met documenten);
- Diefstal van persoonsgegevens als gevolg van een digitale inbraak;
- Hacken en het vervolgens versleutelen van emailaccounts, bestanden en databases (ransomware);
- Versturen van brief of mail met persoonsgegevens naar een verkeerde persoon of organisatie;
- Een boze oud-werknemer ontvreemd data (inclusief persoonsgegevens);
- Persoonsgegevens die onbedoeld benaderbaar waren door een fout in de website;
- Verlies data door brand in het datacenter en er is geen actuele back-up van de persoonsgegevens.

Risico's / Gevolgen / Beheersmaatregelen

Risico's	(Mogelijke) gevolgen	Beheersmaatregelen
Inbreuk op de vertrouwelijkheid Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.	• Nadelige gevolgen voor de betrokkenen, zoals identiteitsfraude; reputatieschade en verlies van vertrouwelijkheid; • Nadelige gevolgen voor OCW, zoals een verminderd vertrouwen van de burger, imagoschade, negatieve publiciteit, en handhavende acties van de toezichthouder (zoals onderzoek en boetes).	• Voorkomen van datalekken door: o bewuste omgang met de data en apparatuur; o de informatiebeveiliging op orde houden van de gebruikte applicaties; • Beperken schade: weten hoe men moet handelen bij een vermoeden van een datalek; • Goede afspraken met verwerkers/leveranciers over beveiliging en melden datalekken; • Afstemming met directie O&B en DUO (Helpdesk O&B) zodat zij melders van beveiligingsincidenten ook wijzen op meldplicht & procedure datalekken; • P&C-cyclus met rapportages over de datalekken en de informatiebeveiliging.
Inbreuk op de integriteit	Vertrouwen neemt af dat besluiten en beslissingen op de juiste wijze genomen zijn/worden.	Beheersmaatregelen die met name zien op een goede informatiebeveiliging.
Inbreuk op de beschikbaarheid	Vertrouwen neemt af dat besluiten en beslissingen op de juiste wijze genomen zijn/worden. Problemen met de Archiefwet.	Beheersmaatregelen die met name zien op een goed continuïteits-beleid.

Betrokken functionarissen/rollen
- Directeuren beleids- en stafdirecties: hebben integrale verantwoordelijkheid voor privacy binnen hun directie en zijn verantwoordelijk voor de naleving van het OCW-brede privacybeleid. De directeur is verwerkingsverantwoordelijk en heeft daarmee de primair verantwoordelijkheid voor het correct naleven van de meldings- en registratieplicht Datalekken.
- Ontdekker van het datalek:
  De persoon die een (mogelijk) datalek ontdekt kan een OCW- medewerker zijn, maar het kan ook een verwerker[3], of een betrokkene[4], de interne ICT-leverancier (DUO) of een externe partij[5].

[3] Een verwerker is een partij die geen onderdeel is van OCW maar in opdracht van OCW verwerkingen van persoonsgegevens uitvoert, waarbij OCW doel en middelen van die verwerking

- Privacy contactpersoon van de directie (PC):
  De PC is aanspreekpunt binnen de directie voor de AIP en de FG. Tevens is hij/zij contactpersoon voor de directie: kent de AVG-procedures, beantwoordt vragen en kan collega's doorverwijzen.
- Functionaris Gegevensbescherming (FG):
  De directie is verplicht om de FG te consulteren[6] . De FG helpt bij het maken van de inschatting van het risico en adviseert over de afhandeling van het datalek. Daarnaast kan de FG zo nodig andere functionarissen betrekken, zoals de CISO en de BVA. De FG registreert de melding in het Register Datalekken (RD). Verantwoordelijkheid als interne toezichthouder om de datelekregistratie regelmatig te bespreken op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check-learn-act cyclus. Zo kunnen organisaties leren van fouten. De functie van FG is ondergebracht bij de directie Bestuursondersteuning en Advies (BOA).
- Adviseur Informatiebeveiliging en Privacy (AIP):
  De AIP is verantwoordelijk voor het opstellen, het laten vaststellen en het herzien van deze AVG procedure. De AIP heeft ook een verantwoordelijkheid voor het evalueren van de procedure en het ophalen van cijfers ten behoeve van rapportage aan het management. De AIP fungeert daarnaast als achtervang voor de FG v.w.b. zijn/haar taken in het kader van deze procedure. De AIP neemt de procedure Datalekken en 'hoe herken ik een datalek?' op in de communicatie- en bewustwordingsactiviteiten. Ondersteunen FG bij het regelmatig bespreekbaar maken van de datalekregistratie op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check-learn-act cyclus. De functie van AIP is ondergebracht bij de directie Bestuursondersteuning en Advies (BOA).
- Beveiligingsambtenaar BD (BVA):
  De BVA krijgt inzage in aantallen en aard van de datalekken die plaatsvinden onder de verwerkingsverantwoordelijkheid van het Bestuursdepartement, t.b.v. van zijn verantwoordelijkheid voor de integrale veiligheid van personen en informatie. Daarnaast ontvangt de BVA een melding wanneer een datalek óók gerubriceerde informatie (of gerubriceerde systemen of apparaten) betreft (ref. VIR-BI). In die gevallen heeft de BVA namelijk een (respons)taak. De functie van BVA is ondergebracht bij de directie Bestuursondersteuning en Advies (BOA).
- Chief Information Security Officer (CISO)
  De CISO kan gevraagd worden om advies over de informatiebeveiligingsaspecten van het datalek. De CISO wordt altijd geïnformeerd bij risicovolle datalekken. De functie van CISO is ondergebracht bij de directie Kennis.
- ICT Servicedesk van DUO: ontvangt meldingen van informatiebeveiligingsincidenten die mogelijkerwijs óók datalekken zijn, maar die per ongeluk niet gemeld zijn bij het meldpuntdatalekken@minocw.nl. Voorbeeld: een medewerker meldt een verloren telefoon zonder zich te realiseren dat er ook persoonsgegevens op stonden van OCW-collega's, zakelijke relaties en/of burgers. Indien er sprake lijkt te zijn van een datalek (in de zin van de AVG), dan neemt de Servicedesk dit op als kenmerk bij de melding en wijst de melder op de meldplicht datalekken (via meldpuntdatalekken@minocw.nl).
- Betrokkene(n): degene van wie gegevens (mogelijk) zijn gelekt.

Rapportages
- Per datalek wordt een formulier ingevuld ten behoeve van het Register Datalekken (RD).

---

bepaalt. In een verwerkersovereenkomst dienen dan ook concrete afspraken gemaakt te worden over het melden van datalekken aan OCW.

[4] Een betrokkene is diegene van wie OCW persoonsgegevens verwerkt. Het kan zijn dat er bijvoorbeeld een datalek plaatsvindt bij het verzenden van (foutief geadresseerde) post of email. De burger in kwestie kan dan in contact treden om aan te geven dat zijn/haar of andermans persoonsgegevens verkeerd terecht gekomen zijn.

[5] Voorbeeld: een responsible disclosure melding (een buitenstaander die online een softwarelek ontdekt en dit meldt, zodat het gedicht kan worden).

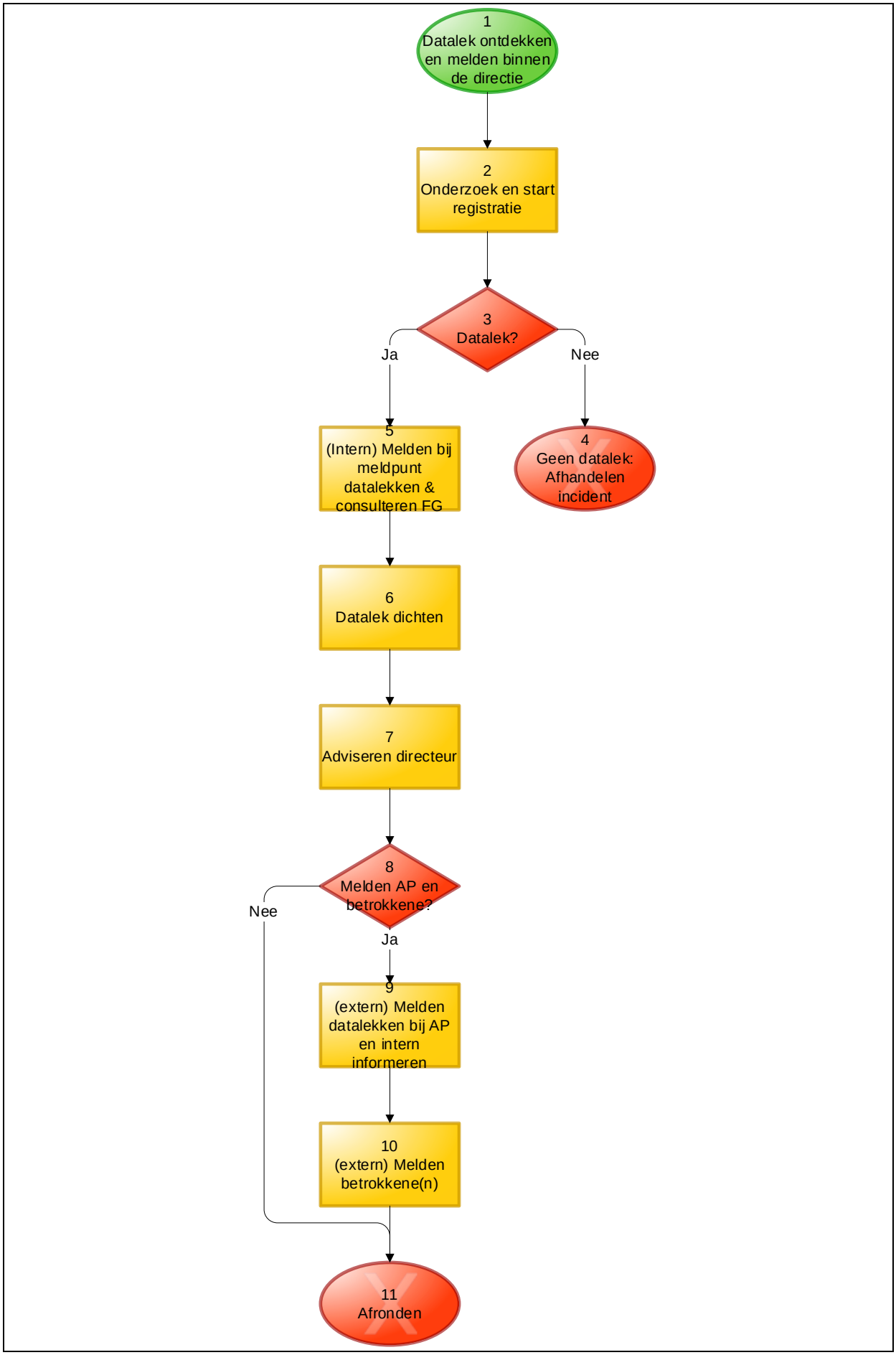
[6] Deze verplichting vloeit niet direct voort uit de AVG. De Europese toezichthouders hebben echter benadrukt dit als concrete uitwerking te zien van Artikel 38 dat vereist dat de verantwoordelijke en de verwerker erop toezien dat de FG "naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens". (…) Daarnaast is het belangrijk dat de FG als een gesprekspartner binnen de organisatie gezien wordt en dat hij of zij deel uitmaakt van de relevante werkgroepen die binnen de organisatie gegevens verwerken. Daarom dient de organisatie er bijvoorbeeld op toe te zien dat (…) de FG dient onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident heeft voorgedaan. Waar nodig kan de verantwoordelijke of verwerker gegevensbeschermingsrichtlijnen of -programma's opstellen waarin aangegeven staat wanneer de FG geraadpleegd dient te worden.

- Per 4 en 8 maanden en jaarlijks rapporteren de organisatieonderdelen aan BOA hoeveel datalekken zijn gemeld, en hoeveel daarvan hebben geleid tot doorzetten naar de AP.
- Centraal meldpunt datalekken (FG & AIP) BOA rapporteert op totaalniveau in de MA-cyclus van BOA aan de SG en apart aan FEZ t.b.v. de bedrijfsvoeringsparagraaf in het Jaarverslag OCW t-1 over aantallen ontvangen datalekmeldingen, waarbij onderscheid wordt gemaakt naar de categorieën 0, 1, 2 en 3.

Centrale rol Bestuursdepartement ten opzichte van heel OCW
Naleving van de AVG valt bij OCW onder de verantwoordelijkheid van de ministers en geldt daarmee voor een ieder die onder de ministeriële verantwoordelijkheid valt. Onderdelen van OCW mogen eigen aanvullend privacybeleid opstellen. Daarbij nemen zij het OCW privacybeleid als raamwerk waarbinnen zij hun eigen privacybeleid en de daaruit volgende procedures nader vormgeven, waaronder een procedure datalekken (bladzijde 13 OCW Privacybeleid).

De organisatieonderdelen die onder het privacybeleid vallen zijn: het Bestuursdepartement, Dienst Uitvoering Onderwijs, Inspectie Erfgoed en Overheidsinformatie, Inspectie voor het Onderwijs, Nationaal Archief, Rijksdienst voor het Cultureel Erfgoed, Adviesraad voor Wetenschap, Technologie en Innovatie, de Onderwijsraad en de Raad voor Cultuur.

Het informeren van de FG OCW bij (meldingswaardige) datalekken is bij alle onderdelen m.u.v. DUO onderdeel van het proces. DUO heeft een eigen FG. Daarnaast leveren alle organisatieonderdelen jaarlijks informatie op aan de directie BOA over aantallen datalekken. Dit heeft als doel om een centraal beeld te vormen van dit aspect van de naleving van de AVG door OCW als geheel.


1
Datalek ontdekken en melden binnen de directie
2
Onderzoek en start registratie
3
Datalek?
Ja
Nee
5
(Intern) Melden bij meldpunt datalekken & consulteren FG
4
Geen datalek: Afhandelen incident
6
Datalek dichten
7
Adviseren directeur
8
Melden AP en betrokkene?
Nee
Ja
9
(extern) Melden datalekken bij AP en intern informeren
10
(extern) Melden betrokkene(n)
11
Afronden

TVB-matrix

	Relaties	Kenmerken
Melden, afhandelen en oplossen datalek	directeur BOA	Proceseigenaar
Datalek ontdekken en melden binnen de directie	ontdekker datalek	Uitvoeren
	privacy contactpersoon (PC)	Uitvoeren
Onderzoek en startregistratie	privacy contactpersoon (PC)	Uitvoeren
	privacy contactpersoon (PC)	Registreren
Datalek?		
Geen datalek: Afhandelen inddent	privacy contactpersoon (PC)	Uitvoeren
	privacy contactpersoon (PC)	Registreren
	privacy contactpersoon (PC)	Informeren
(Intern) Melden bij meldpunt datalekken & consulteren FG	parlementair contactpersoon	Uitvoeren
	parlementair contactpersoon	Informeren
Datalek dichten	privacy contactpersoon (PC)	Uitvoeren
Adviseren directeur	privacy contactpersoon (PC)	Adviseren
Melden AP en betrokkene?		
(extern) Melden datalekken bij AP en intern informeren	directeur	Uitvoeren
	directeur	Informeren
(extern) Melden betrokkene(n)	directeur	Uitvoeren
Afronden	privacy contactpersoon (PC)	Uitvoeren
	functionaris voor gegevensbescherming (FG)	Bewaren

1.1 Datalek ontdekken en melden binnen de directie

Op het moment dat bekend wordt dat er (mogelijk) een datalek heeft voorgedaan, is er sprake van een ontdekker. Het staat de verantwoordelijke directie vrij om te bepalen aan welke functionaris deze meldt. De mogelijkheden zijn:

- de medewerker die binnen de directie verantwoordelijk is voor het desbetreffende proces/ de 'verwerking' waarbinnen het datalek zich voordeed;
- de privacy contactpersoon (PC) van de directie;
- Het kan ook een tweetrapsraket zijn waarbij ontdekker meldt bij de verantwoordelijk medewerker, die op zijn/haar beurt de PC informeert.

Vanaf nu wordt er voor het gemak vanuit gegaan dat de PC de melding van het datalek verder afhandelt en de directeur ondersteunt bij zijn/haar verantwoordelijkheid in deze.

1.2 Onderzoek en start registratie

De PC onderzoekt het incident. De belangrijkste informatie over het datalek wordt verzameld. Afhankelijk van waar het datalek plaatsvond, zal de PC in contact moeten treden met interne of externe leveranciers om informatie te verkrijgen.
Stappen:

- Allereerst moet vastgesteld worden of er persoonsgegevens betrokken zijn bij het datalek. Als er géén persoonsgegevens betrokken zijn, maar er is wél sprake van een beveiligingsincident, dan moet de directie verder het OCW IB Incidentenbeleid 2020 van directie O&B volgen en melden aan de ICT Helpdesk (IB Incidentenbeleid OCW) .

- Als er persoonsgegevens betrokken zijn, is het vervolgens met name belangrijk om vast te stellen óf uit te sluiten dat "persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking".
- De PC informeert de directeur.

Let op: soms is een incident een datalek als:
- Niet vaststaat dat er iets onrechtmatigs gebeurd is met persoonsgegevens;
- Maar ook niet uit te sluiten is dat er ongeoorloofde (onrechtmatige) verwerking van persoonsgegevens plaatsgevonden heeft .

Voorbeeld. Te denken valt aan een bestand met persoonsgegevens dat op hele simpele wijze te benaderen is geweest. Bijvoorbeeld omdat het document in Proza geen toegangsbeperkingen heeft. Dat wil zeggen dat het hele departement bij de persoonsgegevens kan ('leesrechten voor heel BD'). Het valt dan moeilijk te bewijzen dat deze persoonsgegevens alleen door die functionarissen is benaderd die deze persoonsgegevens in de uitoefening van hun functie nodig hadden. Tenzij men de hele geschiedenis via de logfiles gaat onderzoeken om onrechtmatige inzage uit te kunnen sluiten, moet in dit voorbeeld worden uitgegaan worden van een datalek.

Er wordt een start gemaakt met de registratie middels het formulier melden datalekken Meldingsformulier datalek .
De PC registreert de gegevens rond het (vermoedelijke) datalek. Welke gegevens geregistreerd moeten worden, staat in het formulier, deel 1 (zie ook de bijlage). De PC slaat deze eerste versie van het formulier op in Proza. Waarschijnlijk is nog niet alle informatie aanwezig om het formulier volledig in te kunnen vullen. Elke keer wanneer belangrijke nieuwe informatie bekend wordt, past de PC het formulier aan. Vanaf processtap 2.4 wordt de laatste versie van het formulier verstrekt aan de FG via het mailto:meldpuntdatalekken@minocw.nl.

1.3 Datalek?

Als het geen datalek betreft: zie activiteit Geen datalek: Afhandelen incident
Is er sprake van een datalek: zie activiteit: (Intern) Melden bij meldpunt datalekken & consulteren FG

N.B. Indien de PC moeite heeft de benodigde informatie te verkrijgen binnen deze tijdslijnen, bijvoorbeeld doordat verantwoordelijke proceseigenaar, contactpersoon van externe organisaties, of (andere) materiedeskundigen zoals de FG niet bereikt kunnen worden voor overleg, of doordat zij de benodigde informatie niet leveren, escaleert de PC naar de eigen directeur. Dit omdat het verantwoordelijkheid van de directeur is, dat op juiste en tijdige wijze wordt voldaan aan de meld- en registerplicht. Het is aan te raden om bij twijfel een voorlopige melding aan de AP te doen, waarna er tijd is gewonnen om onderzoek te doen en afstemming te zoeken. De voorlopige melding moet wel binnen uiterlijk 2 tot 4 weken aangevuld of teruggetrokken worden.

1.4 Geen datalek: Afhandelen incident

Het is geen datalek als:
- Is vastgesteld dat er geen persoonsgegevens betrokken waren;
- of wanneer redelijkerwijs kan worden uitgesloten dat persoonsgegevens zijn vernietigd, verloren, gewijzigd of ongeoorloofd verstrekt zijn, dan wel ongeoorloofd toegang is verstrekt.

De PC past het formulier melding (vermoedelijk) datalek –deel 2 aan en stuurt het wederom naar het Meldpuntdatalekken@minocw.nl. De FG verwerkt het formulier in het register (RD). Hiermee is de melding afgehandeld en heeft het een 0-categorie meegekregen. De PC informeert de directeur. De PC zorgt vervolgens dat het incident (niet zijnde een datalek) verder wordt afgehandeld en zet zo nodig acties uit conform het OCW IB Incidentenbeleid 2020; zie eerder genoemde link.

1.5 (Intern) Melden bij meldpunt datalekken & consulteren FG

De directie doet zo snel mogelijk maar uiterlijk binnen 24 uur melding van een datalek bij meldpuntdatalekken@minocw.nl, met een cc aan de eigen directeur. Hierbij verstrekt de PC het formulier als bijlage (deel 1 & 3 zo compleet mogelijk ingevuld). Doel:

- Consulteren FG om gezamenlijk te bepalen wat de aard van het risico is t.b.v. het voldoen aan de meldplicht datalekken en;
- Om als bestuursdepartement een centraal datalekregister aan te leggen en daarmee te voldoen aan de registerplicht;

Let op: het kan zijn dat in deze fase (binnen 24 uur na ontdekken) nog niet helemaal duidelijk is óf het wel een datalek betreft. Stelregel is: intern melden als binnen die 24 uur niet uitgesloten kan worden dat persoonsgegevens zijn vernietigd, verloren zijn gegaan, gewijzigd of ongeoorloofd verstrekt zijn dan wel ongeoorloofd toegang is verstrekt.

De PC en de FG stellen samen vast of het inderdaad een datalek betreft. Vervolgens wordt onderzocht hoe ernstig het datalek is. Zo nodig wordt de Chief Information Security Officer (CISO) betrokken en/of andere experts. Daarbij wordt bepaald welke categorie het betreft:

0. Het is geen datalek;
1. Het is een datalek, maar het is uitgesloten dat het een risico opgeleverd heeft voor betrokkene(n) . Let op: alle datalekken moeten worden opgenomen in het register. Dus ook wanneer niet gemeld hoeft te worden aan de AP en betrokkenen.
2. Het datalek is risicovol is voor de betrokkene(n). Dan moet gemeld worden aan AP;
3. Het datalek houdt een hoog risico in voor de betrokkene(n). Dan moet gemeld worden aan AP én betrokkenen.

1.6 Datalek dichten

Tegelijkertijd met stap 5 (intern melden van het datalek) zet de verantwoordelijke directie acties uit om de oorzaken van het datalek aan te pakken. Het kan zijn dat de acties uitgezet moeten worden bij de interne of externe dienstenleverancier:

a) Wanneer het de interne ICT van het bestuursdepartement betreft, dan moet hier de OCW IB Incidentenbeleid 2020 van de directie O&B gevolgd worden;
b) Wanneer het een externe leverancier betreft wordt gehandeld in lijn met de afspraken in de eventuele **verwerkersovereenkoms**t. Dat wil zeggen: de verwerker die het datalek ontdekt neemt zo snel mogelijk maar uiterlijk binnen 24 uur contact op met zijn/haar contactpersoon bij het ministerie. De verwerker dicht het datalek. De verwerker verleent medewerking zodat de directeur de meldplicht datalekken tijdig en volledig kan naleven. Ten slotte verstrekt de verwerker alle informatie die nodig is om te voldoen aan de datalekkenregisterplicht.
c) Wanneer het een andere overheid betreft, worden afspraken nageleefd die zijn vastgelegd in respectievelijk **verwerkingsafspraken** (de andere overheid is verwerker) of een **artikel 26 overeenkomst** (zowel de andere overheid als OCW zijn beiden verwerkingsverantwoordelijke). In het eerste geval zijn er afspraken in lijn met b. In het tweede geval is op schrift gesteld wie van de twee partijen een datalek afhandelt en zo nodig meldt bij de AP en de betrokkenen.

1.7 Adviseren directeur

De PC stelt een advies op voor de directeur, op basis van de consultatie van de FG en eventuele anderen:

- Over de afhandeling van het datalek zelf;
- Over de ernst van het datalek;
- Of het datalek moet worden gemeld aan de AP en zo ja, of het dan ook gemeld moet worden aan de betrokkene(n);

Let op: als er door verschil in inzicht geen gezamenlijk advies bereikt kan worden, stelt de FG een apart advies op voor de directeur.
De directeur bepaalt of het datalek gemeld wordt bij de Autoriteit Persoonsgegevens. Redenen om niet te melden zijn:

1. als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen.

2. Of omdat de organisatie dermate stevige beveiligingsmaatregelen heeft getroffen voordat het datalek plaatsvond, zodat de persoonsgegevens onbegrijpelijk zijn voor buitenstaanders (door bijvoorbeeld versleuteling van de gegevens).
3. Het kan ook zijn dat de persoonsgegevens naar de verkeerde persoon zijn gestuurd, maar dat deze onjuiste ontvanger betrouwbaar is.
   Belangrijke hulpmiddelen:

- De AP biedt een handvat om deze beslissing te vergemakkelijken: Meldplicht datalekken;
- Het meest gezaghebbende document zijn de guidelines (richtlijnen) van de European Data Protection Board (EDPB) over datalekmeldingen. In de guidelines staat een lijst met veel voorkomende soorten datalekken. Zoals ransomware-aanvallen en zoekgeraakte of gestolen apparatuur. Per categorie staat aangegeven welke maatregelen een organisatie van tevoren had moeten nemen. En welke maatregelen de organisatie na het incident moet nemen.

N.B. Indien niet tijdig voldoende informatie beschikbaar is om een volledige melding te doen bij de Autoriteit Persoonsgegevens (AP), wordt besloten om een voorlopige melding te doen. Deze kan bij voortschrijdend inzicht later aangepast of ingetrokken worden.

1.8 Melden AP en betrokkene?

Indien melding aan AP en betrokken(e): zie activiteit (extern) Melden datalekken bij AP en intern informeren.
Indien geen melding plaatsvindt: zie activiteit Afronden.

1.9 (extern) Melden datalekken bij AP en intern informeren

De melding van een inbreuk aan de AP is verplicht, tenzij het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. De directeur van de betreffende directie draagt er zorg voor dat uiterlijk 72 uur na ontdekking van het datalek, deze wordt gemeld bij de Autoriteit Persoonsgegevens (AP). Wanneer nodig kan ondersteuning worden gevraagd bij de AIP of FG (beide BOA).
De directeur wijst een medewerker aan die het meldingsplichtige datalek meldt aan de Autoriteit Persoonsgegevens via het voorgeschreven webformulier Autoriteit persoonsgegevens - Meldloket.
N.B. Indien niet tijdig voldoende informatie beschikbaar is om een volledige melding te doen bij de Autoriteit Persoonsgegevens, wordt binnen 72 uur een voorlopige melding gedaan. Deze melding wordt binnen redelijke termijn (2 tot 4 weken) definitief gemaakt of ingetrokken.

Intern informeren:

- De FG (via meldplichtdatalekken@minocw.nl) en de CISO worden **altijd** geïnformeerd na melding bij de AP;
- Zo nodig, afhankelijk van de ernst en gevoeligheid van het datalek, informeert de directeur de DG en SG.
- De beveiligingsambtenaar (BVA) wordt geïnformeerd als het datalek ook gerubriceerde informatie, systemen of apparaten betreft;
- Wanneer een datalek een crisis tot gevolg heeft of kan hebben, treden de bestaande crisisprocedures in werking. De directeur van de verantwoordelijke directie of de directeur BOA kan daartoe besluiten.
- Als het (ook) een beveiligingsincident is, die onder de verantwoordelijkheid van het OCW IB Incidentenbeleid 2020 valt, dan wordt de directeur O&B geïnformeerd.

1.10(extern) Melden betrokkene(n)

Bij datalekken met een hoog risico voor de betrokkenen, meldt de directeur het datalek ook aan de personen van wie de gegevens zijn gelekt. Dit hoeft alleen als:

1. het datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert. Er moet dan gekeken worden of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade. Kan aannemelijk gemaakt worden dat dit niet zo is? Dan hoeft het datalek niet aan de betrokkenen gemeld te worden.
2. Maatregelen die genomen worden nadat het datalek plaatsvond, kunnen zorgen voor een dermate reductie van het risico dat melding niet meer nodig is. Bijvoorbeeld omdat meteen

actie is ondernomen, waardoor de persoon die toegang had tot de persoonsgegevens er niks mee heeft gedaan.
3. Daarnaast noemt de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) een geval waarbij melding aan betrokkenen achterwege mag blijven: wanneer 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 kinderen een hulpvraag hebben gedaan zonder dat hun ouders dat weten.

De hulpbronnen van de AP geven nader richting bij het bepalen wanneer het wel nodig is (hoofdstuk 3 en 4 van eerder genoemde guidelines meldplicht datalekken). De directeur kan hier ook advies over inwinnen bij de FG en de AIP.

Zou het individueel informeren van de betrokkenen een onevenredige inspanning vergen? Bijvoorbeeld omdat de contactgegevens van de betrokkenen zijn verloren door het datalek? In dat geval voldoet een openbare mededeling.

Betrek een Senior Communicatie Adviseur van de directie Communicatie en de FG bij het opstellen van een brief of andersoortige mededeling aan betrokkenen.

1.11 Afronden

De PC rondt het datalek administratief af:
- Stelt vast dat het datalek gedicht is en de procedure naar tevredenheid is afgerond.
- Werkt zo nodig de gegevens rond de melding in het meldingsformulier bij;
- Licht de ontdekker van het datalek in;
- Stuurt het definitieve formulier op naar het meldpunt datalekken;
- Rondt e.a. af met directeur en met eventuele interne of externe dienstenleveranciers die betrokkenheid hadden bij het datalek.

De FG neemt het definitieve formulier op in het Register van Datalekken (RD).