

Procedure melding en afhandeling datalek

Inleiding

Dit document beschrijft de verschillende stappen die binnen het Regionaal Archief Zuid-Utrecht (RAZU) genomen worden bij een (vermoedelijk) datalek, welke valt onder de registratie en mogelijke meldplicht datalekken van de Algemene Verordening Gegevensbescherming (AVG). Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in 33 en 34 AVG). De persoonsgegevens zijn dan (mogelijk) blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen onder meer ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, virus/malware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden, het verstrekken van inlognaam/wachtwoord aan derden, incorrecte autorisaties);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email naar onjuiste geadresseerden;
- maar ook het onrechtmatige verwerking van gegevens.

Een datalek dient intern gemeld, geregistreerd en beoordeeld te worden. Afhankelijk van de beoordeling worden maatregelen geadviseerd. Deze maatregelen dienen te worden gemonitord door de informatiemanager. Uit de beoordeling volgt ook of het datalek dient te worden gemeld bij de Autoriteit Persoonsgegevens (AP) en of de betrokkenen moeten worden geïnformeerd.

Rollen

1. Datalek behandelteam

Het Datalek behandelteam bestaat uit

- Functionaris voor de Gegevensbescherming (FG)
- Informatiemanager (IM)
- Directeur-archivaris (DA)
- Adjunct-archivaris (AA)
- Contactpersoon ICT Dienstverlener (CID) (enkel indien MS365 omgeving of ICT infrastructuur betrokken is bij het datalek)

2. Behandelaar

De informatiemanager is primaire behandelaar van datalekken. In zijn afwezigheid wijst de directeur-archivaris een vervanger aan. De behandelaar is verantwoordelijk voor het ontvangen en behandelen van meldingen van vermoedelijke datalekken, wat onder meer omvat: het bijeenroepen van het Datalek behandelteam, het opstellen van een advies voor de verwerkingsverantwoordelijke en het doen van een melding bij de autoriteit persoonsgegevens.

3. (Verwerkings-)verantwoordelijke

De verwerkingsverantwoordelijke is degene die formeel, juridisch en feitelijk zeggenschap heeft over het doel en de middelen voor de verwerking van persoonsgegevens en daarmee ook de verantwoordelijke voor het proces waarbinnen het datalek plaatsvindt. De verwerkingsverantwoordelijke is het bestuur van het Regionaal

Archief Zuid-Utrecht. Op basis van de mandaatregeling RAZU 2022 treedt de directeur-archivaris namens het bestuur op als verwerkingsverantwoordelijke. Indien een datalek plaatsvindt in de collectie dan kan er sprake zijn van een deel-verantwoordelijkheid met de zorgdrager van het betreffende onderdeel van de collectie. Het bestuur van het Regionaal Archief Zuid-Utrecht is eindverantwoordelijk.

4. Verwerker

Een externe partij die de gegevens ten behoeve van de verantwoordelijke verwerkt, zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. De verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, etc.

Verwerkers mogen niet zelfstandig (vermoedens tot) datalekken melden bij de Autoriteit Persoonsgegevens, maar dienen te allen tijde het RAZU te informeren, conform de tussen het RAZU en de verwerker afgesloten verwerkersovereenkomst.

Melding aan datalek behandelteam

Elk (mogelijk) datalek dient direct via de behandelaar aan het datalek behandelteam gemeld te worden om de ongewenste situatie te beoordelen en maatregelen te treffen dan wel voor te stellen om deze te herstellen of risico's te beperken. Voor verwerkers en samenwerkende partijen is de verplichting opgenomen in de verwerkersovereenkomst c.q. samenwerkingsovereenkomst.

Melding van een datalek kan worden gedaan door het sturen van een e-mail aan privacy@razu.nl. De melding komt dan terecht bij het datalek behandelteam. Indien een medewerker van het RAZU een melding ontvangt buiten dit kanaal dan moet dit zo spoedig mogelijk worden doorgestuurd.

Intake

De Behandelaar neemt contact op met de melder voor een verdere intake om te beoordelen of er inderdaad sprake is van een datalek

Bij de intake worden de volgende gegevens vastgelegd:

- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens onder de melding vallen;
- om welk aantal en/of gegevensrecords gaat het;
- welke (groepen) personen betrokken zijn bij de melding;
- welke maatregelen door de melder zijn of worden getroffen;
- welke gevolgen er volgens de melder voor de betrokkenen zijn;
- eventueel de contactpersoon namens de melder voor meer informatie.

Bij voorkeur wordt gebruik gemaakt van het intakeformulier (zie Bijlage A).

Dit intakeformulier wordt door de Behandelaar opgenomen in het Datalek Register.

Eerste analyse en directe acties

De Behandelaar beoordeelt of van de inbreuk redelijkerwijs kan worden aangenomen dat er nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden. Bij de eerste analyse wordt bepaald of er andere (deel-)Verwerkingsverantwoordelijken zijn betrokken bij het datalek.

Eventuele directe acties om het datalek te dichten worden tijdens de eerste analyse geïdentificeerd en direct uitgevoerd.

Registratie

Ieder gemeld (mogelijk) datalek dient door de Behandelaar geregistreerd te worden in het totaaloverzicht in het Datalek Register.

Informerende van Verwerkingsverantwoordelijke

De Behandelaar informeert na registratie direct de Directeur-archivaris en eventuele andere (deel-)Verwerkingsverantwoordelijken. Dit gebeurt via het snelste kanaal (telefonisch / via Teams) maar wordt altijd ook schriftelijk of per mail bevestigd door de behandelaar. De Behandelaar beschrijft het incident en stelt de te nemen maatregelen voor, waaronder minimaal het advies om het datalek wel of niet te laten melden bij de AP en het wel of niet informeren van de betrokkenen. De Directeur-archivaris neemt vervolgens het formele besluit om te melden bij de AP. Bij twijfel kan dit besluit worden uitgesteld tot na het overleg met het Datalek behandelteam, mits dit overleg binnen 72 uur na ontdekking van het datalek plaatsvindt.

Overleg

Incidenten met een laag risico, welke niet meldingsplichtig zijn, worden door de behandelaar afgehandeld. Bij een hoog risico of niet precies te duiden datalek kan de Behandelaar besluiten het voltallig Datalek behandelteam bijeen te laten komen. Het Datalek behandelteam wordt altijd bijeengeroepen als andere (deel-)Verwerkingsverantwoordelijken betrokken zijn bij het datalek. De wijze waarop (videoconference, fysiek, e-mail) is afhankelijk van de aard en impact van het potentiële datalek en het tijdstip van de melding.

Tijdens kantooruren: direct bijeenroepen van het Datalek behandelteam,

Buiten kantooruren en in het weekend: Als het mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

De bijeenkomst wordt voorgezeten door de Behandelaar. Het responseteam bespreekt en legt vast:

- de gegevens die door de Behandelaar zijn vastgelegd bij de intake;
- de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en/of tegelijkertijd meer informatie vergaren over de indringer). Deze vervolgacties zullen in het advies aan de Verwerkingsverantwoordelijke worden opgenomen. Het Datalek behandelteam kan besluiten bepaalde risico mitigerende maatregelen al direct in gang te zetten;
- hetgeen gemeld gaat worden bij de AP door de Behandelaar (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records);
- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die het RAZU neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
- de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;

- contactgegevens voor betrokkenen;
- de wijze van afhandeling intern, inclusief communicatie naar melder, het Bestuur en eventuele andere verwerkingsverantwoordelijken;
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- hetgeen intern gecommuniceerd wordt, op welk moment;
- hetgeen extern gecommuniceerd wordt, op welk moment;
- of naast het AP ook andere stakeholders geïnformeerd dienen te worden.

Bij deze bespreking worden zo nodig de Richtsnoeren voor toepassing van artikel 33 en 34 AVG van de Autoriteit Persoonsgegevens betrokken.¹

De uitkomsten van dit overleg, tenminste bestaande uit notulen en afspraken, worden door de Behandelaar opgenomen in het Datalek Register. De uitkomsten worden tevens gedeeld met de Privacy Officer(s) en Functionaris(sen) Gegevensbescherming van eventuele betrokken (deel-) Verwerkingsverantwoordelijken.

Melding aan Autoriteit Persoonsgegevens

Wanneer uit de beoordeling blijkt dat er sprake is van een meldingsplichtig datalek, meldt de Behandelaar (na akkoord van de Directeur-archivaris) binnen 72 uur na de ontdekking van het datalek volgens de aangewezen methode het datalek bij de AP.²

In ieder geval zal gemeld moeten worden:

- de aard van de inbreuk, waaronder betrokken persoonsgegevens, categorieën, aantal betrokkenen, aantal gegevensrecords, betrokken partijen;
- een beschrijving van de te verwachten gevolgen;
- de getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken.

Ontvangstbevestiging

Is er een melding gedaan, dan dient de Behandelaar de webbased ontvangstbevestiging, inclusief inhoudelijk melding, op te slaan als een pdf-bestand. Deze ontvangstbevestiging wordt door de Behandelaar opgenomen in het Datalek Register.

Melding aan betrokkenen

De Behandelaar informeert namens het Regionaal Archief Zuid-Utrecht tijdig de (groepen) betrokkenen.

De Behandelaar informeert de Datalek behandelteam betreffende de status van het informeren van de betrokkenen en verschaft het Datalek behandelteam een geanonimiseerd voorbeeld van het daadwerkelijke verstuurd bericht.

Deze voorbeelden worden door de Behandelaar opgenomen in het Datalek Register voor eventueel nader gebruik.

¹ Deze richtsnoeren voor de melding van datalekken zijn te vinden op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf.

² Zie <https://datalekken.autoriteitpersoonsgegevens.nl>.

Melding aan bestuur

Zodra omvang en impact van het datalek bekend zijn informeert de Directeur-archivaris het voltallige bestuur over het datalek. Indien bij een datalek een groot risico wordt verondersteld geschied het informeren direct. Bij minder risicovolle datalekken geschiedt dit via een rapportage in de eerst volgende bestuursvergadering.

Bij een melding bij het bestuur wordt in ieder geval ingegaan op:

- de aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- een beschrijving van de te verwachten gevolgen;
- de getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- de contactgegevens voor de betrokkene(n).

Bijlage A: intakeformulier datalek (ook digitaal beschikbaar als Microsoft Forms formulier)

Melding door:	Intake door:
Datum melding:	Intake met:
Vorm melding:	Datum intake:
Vorm intake:	Beoordeling:

Vragen te stellen bij intake melding mogelijk datalek (persoonlijk of telefonisch contact)

1. Noteer gegevens van de melder en/of betrokkene, naam en bereikbaarheidsgegevens:

2. Wat is de aard van de inbreuk? (meerdere mogelijkheden aankruisen/beschrijven.)
 - ☐ Lezen (vertrouwelijkheid)
 - ☐ Kopiëren
 - ☐ Veranderen (integriteit)
 - ☐ Verwijderen of vernietigen (beschikbaarheid)
 - ☐ Diefstal
 - ☐ Verloren
 - ☐ Nog niet bekend
 - ☐ Anders / Omschrijving van de situatie:

3. Zijn gegevens nog ergens anders of op een andere manier beschikbaar?

4. Gevolgen van wel/niet beschikbaar hebben in andere vorm?

5. Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
 - ☐ Op _____
 - ☐ Tussen _____ en _____
 - ☐ Nog niet bekend

6. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

7. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in)

Minimaal: _____

Maximaal: _____

8. Om welk type persoonsgegevens gaat het? (U kunt meerdere mogelijkheden aankruisen.)

- ☐ Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG: Godsdienst, levensovertuiging,
- ☐ ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens
- ☐ Gegevens over de financiële of economische situatie van de betrokkene
- ☐ (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
- ☐ Gebruikersnamen, wachtwoorden en andere inloggegevens
- ☐ Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer
- ☐ om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).
- ☐ Naam-, adres- en woonplaatsgegevens
- ☐ Telefoonnummers
- ☐ E-mailadressen of andere adressen voor elektronische communicatie
- ☐ Geslacht, geboortedatum en/of leeftijd
- ☐ Anders: _____

9. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

10. Voorstel structurele verbeteringen / Overig advies:

In te vullen door de behandelaar

Eerste indruk bij intake, bekeken vanuit impact voor betrokkenen (aankruisen wat van toepassing)

- ☐ Nihil risico
- ☐ Verwaarloosbaar risico
- ☐ Substantieel risico
- ☐ Hoog risico

Aantekeningen:

Bijlage B

Stroomdiagram

Procedure Datalek Behandelen

