Procedure melding en afhandeling datalek

1. Inleiding

Dit document beschrijft de verschillende stappen die binnen Tilburg University (TiU) genomen worden bij een datalek, die 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.
Uit de beoordeling volgt ook of het datalek dient te worden gemeld bij de Autoriteit Persoonsgegevens (AP) en of de betrokkenen moeten worden geïnformeerd.

2. Rollen

i. Responseteam Datalek

Het Responseteam Datalek bestaat uit

1) Functionaris voor de Gegevensbescherming (FG)
2) Centrale Privacy Officer (CPO)
3) Governance Risk Compliance Officer (GRC)
4) IT Security Officer (ITSO)
5) CERT-medewerker(s)
6) Chief Information Security Officer (CISO)
7) Privacy specialist van Juridische Zaken (LA)

ii. Behandelaar

De volgorde van het Responseteam Datalek bepaalt wie de melding initieel aanneemt.
Bij afwezigheid dient de volgende collega uit het Responseteam Datalek de melding aan te nemen.

iii. (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. Dit is in de regel de directeur van de betreffende divisie of School. Ter illustratie: wanneer een medewerker van divisie X werkzaamheden uitvoert binnen een proces van School Y, dan is de verantwoordelijke voor een datalek binnen dat proces de directeur van School Y.

Het College van Bestuur is eindverantwoordelijk.

iv. **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.

3. Melding aan Responseteam Datalek

Elk (mogelijk) datalek dient direct aan het Responseteam Datalek 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. Deze verplichting is voor medewerkers vastgelegd en gecommuniceerd via het protocol 'meldplicht datalekken'[1]. 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 datalek@tilburguniversity.edu, de melding komt dan terecht bij het Responseteam Datalek.

De melding kan ook door een externe persoon worden gedaan bij een medewerker van TiU. De melding moet dan direct door de medewerker worden doorgezet via een e-mail naar: datalek@tilburguniversity.edu, de melding komt dan terecht bij het Responseteam Datalek.

4. Intake

De Behandelaar neemt contact op met de melder voor een verder 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;
- de contactpersoon voor de melding 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.[2]

[1] www.tilburguniversity.edu/nl/privacy/
[2] Op het moment van schrijven bevindt het Datalek Register zich op de netwerkschijf van de afdeling Executive Support: Internal Audit en Compliance.

5. Eerste analyse

De Behandelaar beoordeelt of van de inbreuk redelijkerwijs kan worden aangenomen dat deze leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden.

6. Registratie

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

7. Informeren van Verwerkingsverantwoordelijke

Afhankelijk van het risico van het datalek informeert de Behandelaar de Verwerkingsverantwoordelijke, telefonisch dan wel schriftelijk, voorafgaand aan het advies, dit omdat de tijd tussen melding en advies te lang zou kunnen zijn .

8. Overleg

Bij een hoog risico of niet precies te duiden datalek kan de Behandelaar besluiten het voltallig Responseteam Datalek bijeen te laten komen, 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 Responseteam Datalek,
Buiten kantoortijden 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 Responseteam Datalek 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 TiU 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, betreffende afdeling(-en), manager(s), directeuren, en indien noodzakelijk het College van Bestuur;
- 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; in overleg met de perswoordvoerder;
- hetgeen extern gecommuniceerd wordt, op welk moment; in overleg met de perswoordvoerder;
- of naast het AP ook andere stakeholders geïnformeerd dienen te worden; in overleg met de perswoordvoerder.

Bij deze bespreking worden zo nodig de Richtsnoeren voor toepassing van artikel 33 en 34 AVG van de Autoriteit Persoonsgegevens betrokken.[3]

9. Advies aan Verwerkingsverantwoordelijke

De Behandelaar adviseert de Verwerkingsverantwoordelijke schriftelijk. Dit advies 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 Autoriteit Persoonsgegevens en het wel of niet informeren van de betrokkenen. De Behandelaar vraagt ten slotte de Verwerkingsverantwoordelijke om binnen 8 uur na het advies te reageren op dit advies, waarbij de Verwerkingsverantwoordelijke in ieder geval laat weten of de geadviseerde maatregelen worden opgevolgd en zo niet, waarom hiervan wordt afgeweken. Tevens moet de Verwerkingsverantwoordelijke akkoord geven voor het melden van het datalek bij de Autoriteit Persoonsgegevens, indien is beoordeeld dat het een meldingsplichtig datalek betreft.

Dit advies wordt door de Behandelaar opgenomen in het Datalek Register[4]

Escalatie
Indien de Verwerkingsverantwoordelijke besluit af te wijken van de geadviseerde maatregelen, of niet tijdig reageert, kan de FG, GRC of CISO escaleren naar het College van Bestuur.

10. Melding aan Autoriteit Persoonsgegevens

Wanneer uit de beoordeling blijkt dat er sprake is van een meldingsplichtig datalek, meldt de Behandelaar (na akkoord van de Verwerkingsverantwoordelijke) binnen 72 uur na de ontdekking van het datalek volgens de aangewezen methode[5] het datalek bij de Autoriteit Persoonsgegevens. Het beleggen van het daadwerkelijk melden bij de Behandelaar in plaats van bij de Verwerkingsverantwoordelijke is gedaan omwille van expertise en breder zicht op andere lopende of geplande maatregelen.

In ieder geval zal gemeld moeten worden:
- 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).

[3] Deze richtsnoeren voor de melding van datalekken zijn te vinden op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf.
[4] Op het moment van schrijven bevindt het Datalek Register zich op de netwerkschrijf van de afdeling Executive Support: Internal Audit en Compliance.
[5] Zie https://datalekken.autoriteitpersoonsgegevens.nl.

Ontvangstbevestiging

Is er een melding gedaan, dan dient de Behandelaar de webbased ontvangstbevestiging[6], inclusief inhoudelijk melding, op te slaan naar een pdf-bestand.

Deze ontvangstbevestiging wordt door de Behandelaar opgenomen in het Datalek Register.

11. Melding aan betrokkenen

De Behandelaar adviseert de Verwerkingsverantwoordelijke over het informeren van (groepen) betrokkenen. De Verwerkingsverantwoordelijke is verantwoordelijk voor het tijdig informeren van de betrokkenen.

Het Register Datalek bevat te gebruiken templates welke aan de Verwerkingsverantwoordelijke aangeboden kunnen worden.

De Verwerkingsverantwoordelijke informeert de Behandelaar betreffende de status van het informeren van de betrokkenen en verschaft Behandelaar een geanonimiseerd voorbeeld van het daadwerkelijke verstuurde bericht.

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

[6] Op het moment van schrijven wordt door de Autoriteit Persoonsgegevens niet automatisch een ontvangstbevestiging verzonden. Het handmatig opslaan van de webpagina naar een pdf-bestand direct na de melding is daarom vereist.

Documentbeheer				
Versie	**datum**	**distributie**	**status**	**wijzigingen op hoofdpunten**
1.0	01-01-2016	intranet	definitief	n.v.t.
2.0	12-10-2020	intranet	definitief	Herschreven naar huidige situatie AVG. Meldplicht uit WBP naar registratieplicht en conditionele meldplicht uit AVG

Bijlage A: intakeformulier datalek[7]

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

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:

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

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

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

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

   Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
   a) Minimaal:
   b) Maximaal:

5. 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

[7] Meest actuele versies Nederlands en Engels zijn opgenomen in het Register Datalek

☐ (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:

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

Voorstel structurele verbeteringen:

Overig advies:

Eerste indruk bij intake
☐ Inbreuk op beveiliging
☐ Mogelijk verlies persoonsgegevens
  ☐ Aanzienlijke kans op ernstige nadelige gevolgen
☐ Verlies persoonsgegevens
  ☐ Aanzienlijke kans op ernstige nadelige gevolgen
  ☐ Ernstige nadelige gevolgen
