Meldplicht datalekken

Document type	Standard Operating Procedure
Document code	SOP-MELD-DATA-LEK-0001
Huidige versie en datum	1.1 d.d. 13-3-2017
Vorige versie	1.0
Original date	28-9-2016
Toepassing	Algemeen, persoonsgegevens
Doelgroep	Medewerkers van het KKC, onderzoekers die namens YOUth onderzoeksdata verzamelen
Auteur(s)	Anna Oleksiak
Recensent(en)	Charlotte Onland, Juliëtte van der Wal, Lilli van Wielink
Validatie	_____ _____ _____ Naam Cohortmanager Datum Handtekening
Samenvatting van veranderingen	Toegevoegd drie voorbeelden van datalekken (sectie 8.3, tekst in het geel gemarkeerd) en één voorbeeld van bijzondere persoonsgegevens (sectie 8.2, tekst in het geel gemarkeerd)

INHOUD

1 AFKORTINGEN EN DEFINITIES

AP	Autoriteit Persoonsgegevens
Beveiligingsincident	Een gebeurtenis die als gevolg heeft of zou kunnen hebben het aantasten van de beschikbaarheid, de vertrouwelijkheid en/of de integriteit van de informatievoorziening. Als voorbeeld kan men denken aan het verlies van een USB-stick, diefstal van een laptop, malware-besmetting, inbraak door een hacker of brand in een datacentrum.
CERT-UU	Computer Emergency Response Team van de Universiteit Utrecht
CISO	Corporate Information Security Officer van de Universiteit Utrecht
Datalek	Toegang tot of vernietiging, wijziging of vrijkomen van **persoonsgegevens** bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook vernietiging of onrechtmatige verwerking van gegevens. Er is sprake van een datalek als er daadwerkelijk een **beveiligingsincident** plaatsvond waarbij **persoonsgegevens** verloren zijn gegaan of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kan zijn. Het beveiligingsincident heeft dus daadwerkelijk gevolgen voor de persoonsgegevens die je verwerkt.
Ernstige datalek	Wbp Artikel 34a lid 1: Een datalek dat leidt tot een aanzienlijke kans op ernstige nadelige gevolgen, dan wel ernstige gevolgen heeft voor de bescherming van de persoonsgegevens.
KKC	KinderKennisCentrum
Persoonsgegeven	Wbp Artikel 1 lid a: Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. *In het geval van het YOUth-onderzoek nemen we aan dat het om alle onderzoeksdata, persoonsgegevens in SLIM en HiX, en medewerkerspersoonsgegevens gaat.*
SLIM	Database in het beheer van het UMCU - Julius Centrum waar de persoonsgegevens voor administratieve doeleinden van de deelnemers aan het YOUth-onderzoek zijn opgeslagen
HiX	Patiëntenregistratiesysteem van het UMCU, waarin deelnemers van het YOUth-onderzoek die een MRI-meting ondergaan in aangemaakt worden.
SOP	Standard Operating Procedure
UMCU	Universitair Medisch Centrum Utrecht
UU	Universiteit Utrecht
Wbp	Wet bescherming persoonsgegevens
YOUth	YOUth-onderzoek naar de ontwikkeling van hersenen en gedrag van opgroeiende kinderen in de regio Utrecht; experimentele data wordt op het terrein van het KKC/UU en UMCU verzameld
95/46/EG	Europese richtlijn bescherming persoonsgegevens

2 INTRODUCTIE

Als student of medewerker van de Universiteit Utrecht moet je elk **beveiligingsincident** of **datalek** melden bij het **Computer Emergency Response Team** van de universiteit (**CERT-UU**). CERT onderzoekt elk beveiligingsincident en coördineert de afhandeling. Als er sprake lijkt van een datalek dat onder de meldplicht (Artikel 34a van de Wbp) valt, wordt het incident doorgegeven aan de **Corporate Information Security Officer** (**CISO**) van de universiteit. Ernstige datalekken moeten door CISO vermeld worden aan Autoriteit Persoonsgegevens. De boete die wordt opgelegd bij het niet voldoen aan de meldplicht kan oplopen tot €820.000.

Bij YOUth worden de onderzoeksdata gepseudonimiseerd opgeslagen. Echter, zolang YOUth de sleutel bewaard, is de koppeling van de natuurlijke persoon (directe persoonsgegevens in SLIM of HiX bij het UMCU) aan de onderzoeksdata makkelijk om uit te voeren. Om deze reden moet de onderzoeksdata met pseudocode beschouwd worden als persoonsgegeven. Daarnaast bevatten sommige vragenlijsten die de deelnemers invullen gevoelige informatie over b.v. hun nationaliteit, godsdienst of gezondheid. Tot slot verzameld YOUth het videomateriaal van de deelnemers wat direct (zonder het persoonsnummer) tot de natuurlijke persoon leidt.

3 DOEL

Deze procedure beschrijft de handelingswijze in het geval van het ontdekken van een (vermoeden van een) datalek. De plicht een (vermoeden van een) datalek te melden geldt voor alle medewerkers zoals bedoeld in punt 4 van dit document en is van toepassing op alle YOUth data die op het terrein van het KKC of UMCU verzameld worden.

4 WETGEVING EN STANDAARDEN

In de Wet bescherming persoonsgegevens (Wbp) zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd. De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). De Wbp is sinds 1 september 2001 van kracht.

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct (uiterlijk binnen 72 uur) een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In sommige gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Niet voldoen aan deze meldplicht kan leiden tot een boete van tot €820.000.

5 VERANTWOORDELIJKHEDEN EN TAKEN

Hoofdonderzoeker	hoofd van YOUth-onderzoek
Cohortmanager	functionele hoofd van YOUth-onderzoek
Datamanager	medewerker van het KKC die de YOUth data beheert
Logistiek manager	medewerker van het KKC die het KKC en onderzoeksfaciliteiten beheert
Medewerker	medewerker van het KKC of een medewerker van de UU of het UMCU die namens YOUth onderzoeksdata verzamelt of verwerkt

6 PROCEDURE

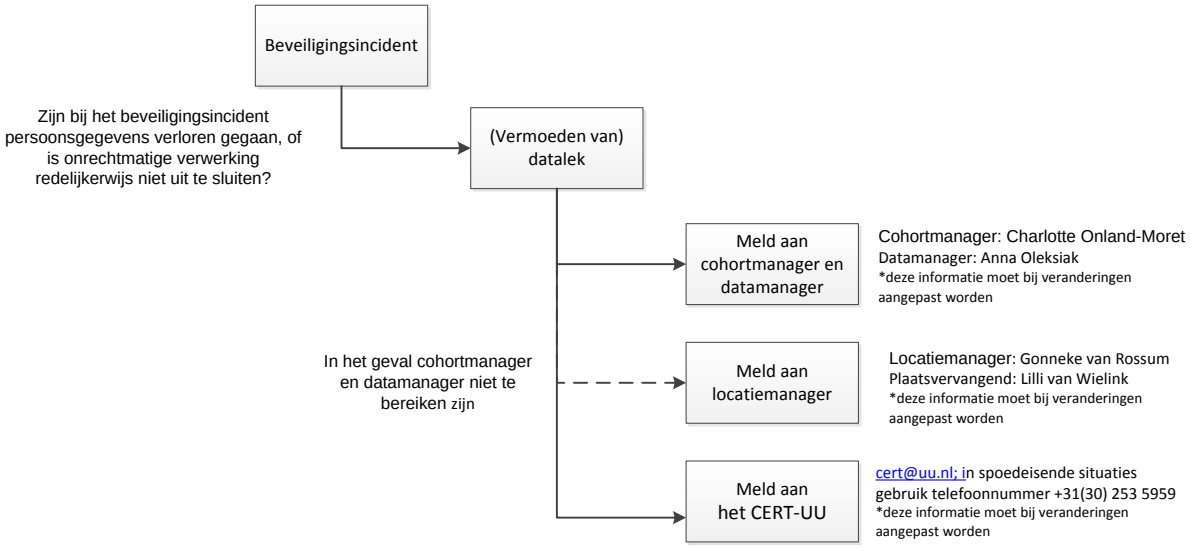
In het geval dat een medewerker een datalek constateert of een datalek vermoedt (voor de definitie zie punt 1 van dit document, voor voorbeelden van een datalek zie punt 8.3), dan is daarop de volgende handelingswijze van toepassing:

- Is er sprake van een datalek of kan een datalek redelijkerwijs niet uitgesloten worden?

Flowchart op basis van ref 2.

- Onmiddellijk na het constateren van een beveiligingsincident en/of een (mogelijk) datalek aan de cohortmanager EN de datamanager doorgeven (in persoon of telefonisch).
- Na het informeren van de cohortmanager en de datamanager, de bevindingen betreffende het beveiligingsincident en/of datalek onmiddellijk versturen naar het CERT-UU via cert@uu.nl. In spoedeisende situaties gebruik telefoonnummer +31(30) 253 5959.

- In het geval de cohortmanager en/of de datamanager zelfs niet telefonisch te bereiken zijn, informeer de locatiemanager; je blijft verplicht het CERT-UU te informeren.
- Plaats de e-mailadressen van de cohortmanager en de datamanager in het CC veld van het bericht naar cert@uu.nl.



De basisinformatie die je aan het CERT-UU in het bericht moet verstrekken:

- Naam van de persoon die meldt
- Functie van de persoon die meldt
- De naam van cohortmanager en hoofdonderzoeker
- E-mailadres van de persoon die meldt
- Telefoonnummer van de persoon die meldt
- Alternatief telefoonnummer van de persoon die meldt
- Gegevens over het beveiligingsincident of/en datalek:
    - Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
    - Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? Geef maximum en minimum aan.
    - Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
    - Wanneer vond de inbreuk plaats? Op (datum) of tussen (begindatum periode) en (einddatum periode) of nog niet bekend.
    - Wat is de aard van de inbreuk? Bijvoorbeeld lezen (vertrouwelijkheid), kopiëren, veranderen (integriteit), verwijderen of vernietigen (beschikbaarheid), diefstal of nog niet bekend.
    - Om welk type persoonsgegevens gaat het? Bijvoorbeeld naam-, adres- en woonplaatsgegevens, telefoonnummers, E-mailadressen of andere adressen voor elektronische communicatie, toegangs- of identificatiegegevens (inlognaam / wachtwoord, persoonsnummer of pseudocode), financiële gegevens (rekeningnummer), geslacht, geboortedatum en/of leeftijd, bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke

overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens), overige gegevens.
- Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? Bijvoorbeeld stigmatisering of uitsluiting, schade aan de gezondheid, blootstelling aan (identiteits)fraude, blootstelling aan spam of phishing.

Als je niet spoedeisende vragen over beveiligingsincidenten of datalekken hebt, kan je contact met CISO opnemen via ciso@uu.nl. Op het moment van schrijven van dit document is René Ritzen (r.ritzen@uu.nl) de aangestelde CISO van de UU.

7 REFERENCES

1 Informatie voor de Universiteit Utrecht Meldplicht datalekken, laatst gewijzigd 9-5-2016: https://intranet.uu.nl/meldplicht-datalekken

2 Richtsnoeren meldplicht datalekken , Autoriteit Persoonsgegevens, 8-12-2015: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf (Beleidsregels voor toepassing van artikel 34a van de Wbp , Vincent Bontrop, 8-12-2015)

3 Wet bescherming persoonsgegevens, geldig vanaf 1-1-2016, gedownload op 28-9-2016: http://wetten.overheid.nl/BWBR0011468/2016-01-01

8 BIJLAGE

8.1 Voorbeelden van persoonsgegevens

- Naam met achternaam
- Geslacht, geboortedatum en/of leeftijd
- Adres en woonplaats
- Postcodes met huisnummers
- Telefoonnummer
- E-mailadres

8.2. Voorbeelden van bijzondere (van gevoelige aard) persoonsgegevens

- Gegevens die betrekking hebben op mensen uit kwetsbare groepen (b.v. kinderen)
- Beeld en geluid
- Gezondheid
- Ras
- Nationaliteit
- Biometrische gegevens (beeldmateriaal, audiomateriaal)
- Biologisch materiaal (haar, wangslijmvlies, speeksel, bloed)
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
- Levensovertuiging

- Seksuele leven
- Gebruikersnamen en wachtwoorden
- Politieke gezindheid
- Cijferlijsten
- Salarisstrookjes
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Lidmaatschap van een vakbond
- Strafrechtelijk verleden
- Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
- BSN-nummer

8.3 Voorbeelden van datalekken

- Verlies of diefstal van een smartphone, laptop, iPad, USB-stick of papieren documenten waarop persoonsgegevens staan
- Inbraak door een hacker tot een bestand met persoonsgegevens
- Papieren documenten met persoonsgegevens onbewaakt laten liggen waarbij de toegang van een onbevoegde redelijkerwijs niet uitgesloten kan worden
- Een computer, laptop of smartphone met persoonsgegevens niet vergrendeld en zonder toezicht laten staan, waarbij de toegang van een onbevoegde redelijkerwijs niet uitgesloten kan worden
- Het kwijtraken van documenten met persoonsgegevens of informatie die naar een persoon kan verwijzen (testdatum, geboortedatum, leeftijd, geslacht – eigenlijk neem aan dat het om alle documentatie in het deelnemers dossier gaat)
- Het kwijtraken van biologisch materiaal afgenomen van een deelnemer
- Het niet ontvangen van het postpakket met speeksel of navelstrengbloed en de vragenlijsten (als de deelnemer beweert dat het pakket was opgestuurd)
- Het niet registreren of retourkomen van vragenlijsten op papier die naar de deelnemers waren verstuurd
- Een e-mail of een brief met persoonsgegevens per ongeluk naar onbevoegde mensen versturen (alle personen binnen onze onderzoeksgroep vallen onder bevoegde personen)
- Verzenden van een groepse-mail waarin de e-mailadressen van de geadresseerde deelnemers in het AAN veld staan en dus leesbaar zijn voor alle geadresseerden
- Een phishing e-mail met een link waarop je klikt en je wachtwoord invoert
- Een andere onderzoeksinstelling gebruikt onze persoonsgegevens buiten de afspraken om voor een ander onderzoek
- Papieren documenten met persoonsgegevens die in een gewone vuilnisbak weggegooid zijn, in plaats van weggooien in de vertrouwelijke papierbak van de UU
- Een computer met persoonsgegevens waarop een malware is ontdekt (sommige typen malware doorzoeken de besmette apparatuur op waardevolle

persoonsgegevens, om de gevonden gegevens op een server te plaatsen die in de handen van de aanvaller is)

- (Onbedoelde) vernietiging van de gegevens zonder dat er een back-up van bestaat (als er een reserve-kopie bestaat, is het geen datalek)
- Een computer met persoonsgegevens, waarvan geen back-up kopieën zijn gemaakt, die door een computervirus (b.v. het geval van ransomware) is geblokkeerd
- Inloggegevens tot een bestand of database aan een onbevoegde onbedoeld verstrekken, waarbij het redelijkerwijs niet uitgesloten kan worden dat deze persoon deze inloggegevens heeft gebruikt voordat de corrigerende maatregels zijn genomen (als de account snel geblokkeerd is en van de logbestanden van de database of server duidelijk is dat deze account in die tijd was niet gebruikt om in te loggen, is het geen datalek).