UT-procedure voor het afhandelen van datalekken
Versie 1.0, 20 November 2017

Als een organisatie zoals de UT een mogelijk datalek ontdekt, dan zal zij snel onderzoek moeten doen, maatregelen nemen en mogelijk ook meldingen moeten doen aan de Autoriteit Persoonsgegevens (AP) en getroffen personen.

Daarom moeten medewerkers van de Universiteit Twente een security incident of een mogelijk datalek zo snel mogelijk melden aan CERT-UT via cert@utwente.nl of Servicedesk ICT (LISA) servicedesk-ict@utwente.nl tel. 5577.

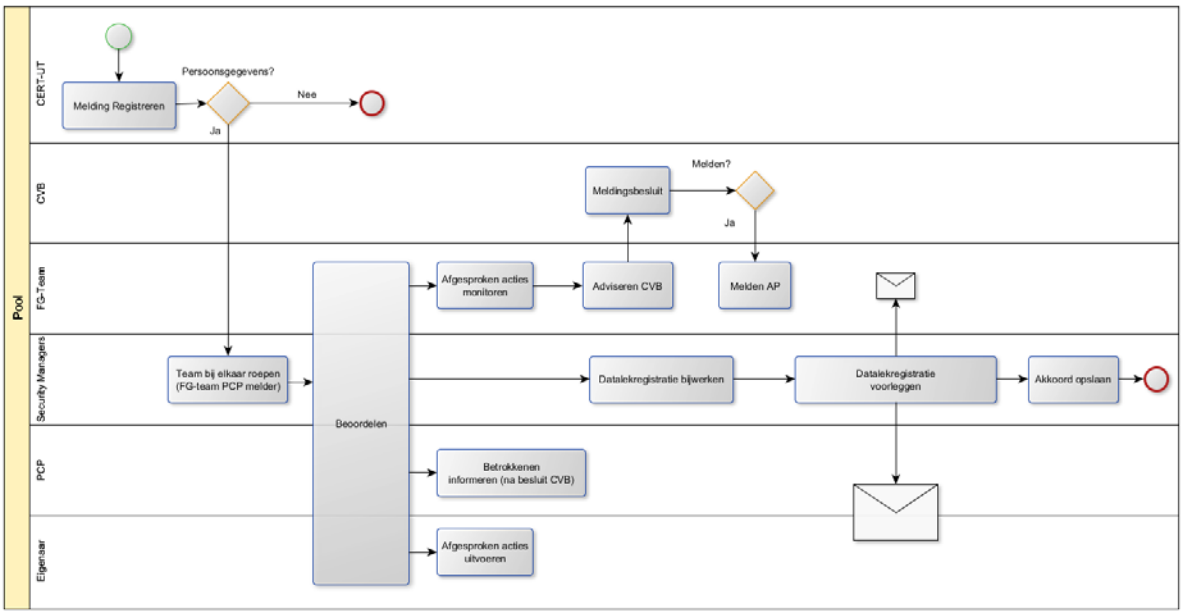
Medewerkers van de ICT Servicedesk zijn alert op mogelijke datalekken zoals: verlies van een USB-stick, de diefstal van een laptop of een inbraak door een hacker. Waar nodig melden zij beveiligingslekken via e-mail aan cert@utwente.nl. In urgente gevallen wordt de dienstdoende CERT-UT medewerker gebeld.

Iedere melding wordt door CERT-UT geregistreerd. Indien nodig neemt CERT-UT contact op met de melder voor aanvullende gegevens over de melding.

Door CERT-UT wordt een eerste analyse gedaan en als het om persoonsgegevens gaat, dan wordt het incident bij de Security Managers van LISA gemeld. De Security Manager verzorgt de afhandeling van het datalek, waarbij bewijsmateriaal of informatie voor het afhandelen van het datalek in een veilige omgeving wordt bewaard.

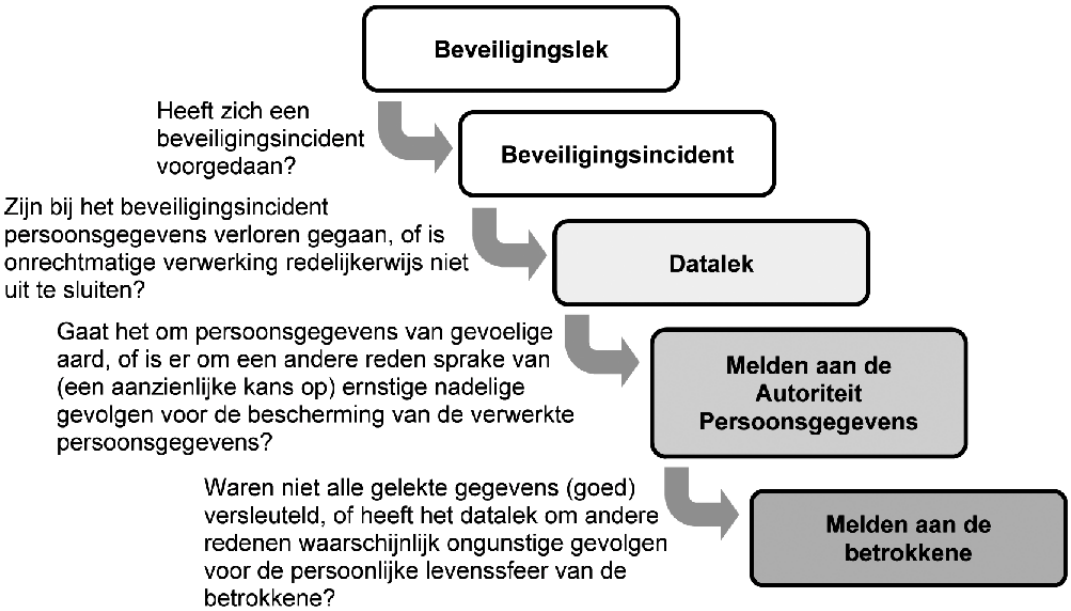
De Security Manager stelt samen met een lid van het FG-team, de Privacy Contact Persoon (PCP) van de betreffende faculteit of dienst en de veroorzaker van het datalek een rapportage en advies op. Hierin wordt advies gegeven aan het CvB-lid verantwoordelijk voor bedrijfsvoering voor wat betreft het melden aan de Autoriteit Persoonsgegevens en het melden aan de betrokkenen (de personen waarvan de persoonsgegevens gelekt zijn). Dit advies wordt door een lid van het FG-team voorgelegd aan het CvB. Het security incident dat ten grondslag ligt aan het datalek wordt verder opgepakt door de Security Manager.

Meldingen bij de AP worden gedaan door een lid van het FG-team, na akkoord van het CvB. Het informeren van de betrokkenen wordt gedaan door de PCP. De Security Manager is verantwoordelijk voor de rapportage. De rapportage wordt ter akkoordverklaring voorgelegd aan de PCP en de veroorzaker van het datalek, middels e-mail. De rapportage en akkoordverklaringen worden door de Security Manager opgeslagen in het datalek-register.



Wanneer melden?

Voor een gedetailleerde beschrijving van de afweging of een melding gedaan moet worden zie Beleidsregels van de Autoriteit Persoonsgegevens. Het onderstaande schema geeft in het kort deze afwegingen weer.



Datalek
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.
Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek.

Melden aan de Autoriteit Persoonsgegevens
Als er sprake is van een beveiligingslek zonder datalek, hoeft deze niet aan de AP te worden gemeld. Maar ook niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Elk gegeven dat herleidbaar is tot een natuurlijk persoon, is een persoonsgegeven. Dit betreft namen, adressen, kentekens, telefoonnummers, IP-nummers, email-adressen, biometrische kenmerken, een combinaties van specifieke voorkeuren.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

- Persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het zelfs mogelijk dat een datalek moet worden gemeld waarbij de persoonsgegevens van slechts één persoon betrokken zijn.

De melding moet worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kan de melding later nog worden aangevuld of ingetrokken.

Melden aan betrokkene
Als een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene. De wet geeft hiervoor als richtlijn dat het datalek moet worden gemeld aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De wet schrijft voor dat de melding aan de betrokkene onverwijld moet worden gedaan, zodat de betrokkene naar aanleiding van de melding maatregelen kan nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd is, hoe eerder deze in actie kan komen.

Als er vooraf passende technische beschermingsmaatregelen waren genomen (zoals encryptie en hashing) waardoor de verloren persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven. Het datalek heeft dan namelijk geen nadelige gevolgen voor de betrokkene.

Rapportage
Kwantitatieve rapportage over datalekken is onderdeel van de securitykwartaalrapportage die door de Security manager van LISA wordt opgesteld.