Protocol datalek voor V.C.M.W. Sigma

In dit document vindt u het protocol wanneer een datalek plaatsvindt in uw vereniging en welke stappen u moet ondernemen. Het is sinds 1 januari 2016 door de Wet bescherming persoonsgegevens (Wbp) verplicht om datalekken te melden. Deze meldplicht geldt zowel voor de betrokkene(n) als bij de Radboud Universiteit te Nijmegen.

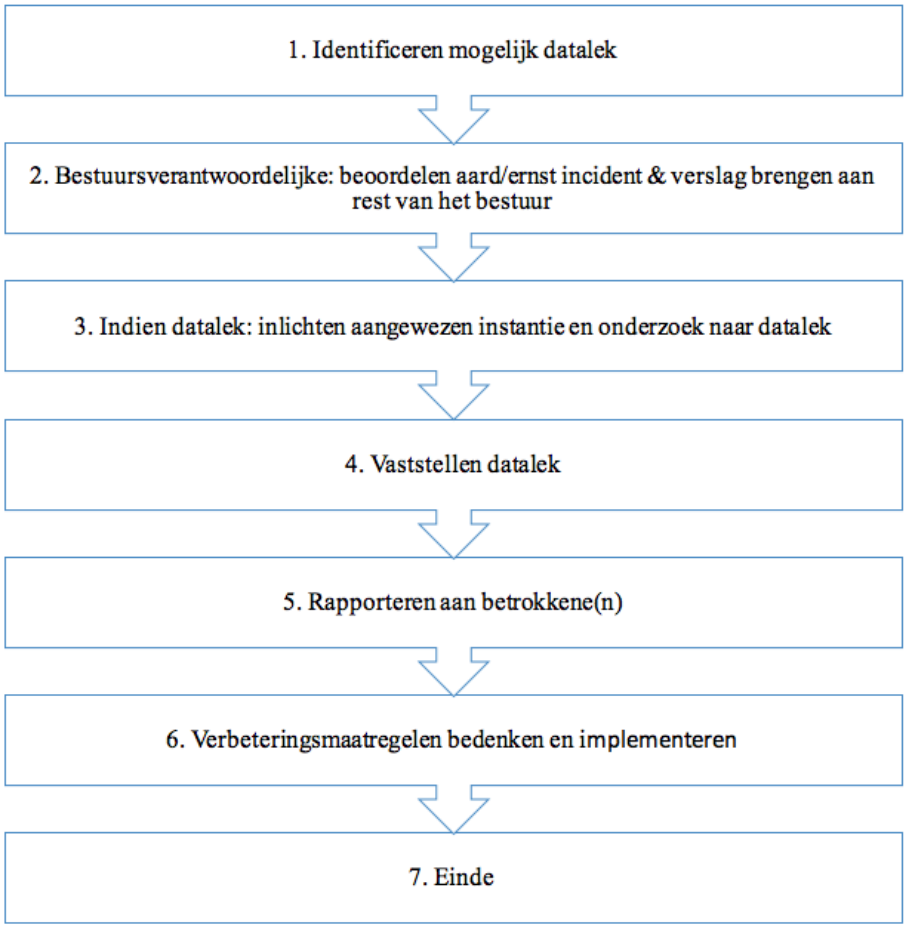
V.C.M.W. Sigma kan per datalek bepalen of de procedure volledig gevolgd moet worden of dat hiervan afgeweken kan worden. Het doel van deze procedure is om vast te leggen welke stappen genomen moeten worden door V.C.M.W. Sigma bij het vermoeden van of kennisnemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek. Hiermee wordt gehoopt dat het volgende resultaat wordt nagestreefd:

- Het steeds volgen van een eenduidige procedure.
- Het zorgvuldig waarborgen van belangen van de studievereniging, het individu dan wel een andere organisatie die betrokken is bij het incident, zijnde (mogelijk) datalek.
- Het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident.
- Het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen.
- Het aanwijzen van een bestuursverantwoordelijke omtrent datalekken en het aanwijzen van een instantie waarbij aangeklopt kan worden bij het ontdekken van een (mogelijk) datalek. Daarbij kan gedacht worden aan een privacycoördinator van de Radboud Universiteit.

Aanpak datalek

Wanneer er dus sprake is van een (mogelijk) datalek dan kan het volgende processchema aangehouden worden (Na het schema zal een uitleg per stap beschreven worden).

z.o.z.



1. Identificeren mogelijk datalek

Indien een (mogelijk) datalek wordt geconstateerd, wordt de rest van het bestuur ingelicht. De bestuursverantwoordelijke voor datalekken bepaalt daarbij of hij/zij het probleem alleen op zich neemt of een ander bestuurslid (of eventueel een oud-bestuurder/actief lid) betrekt in het proces.

2. Bestuursverantwoordelijke; beoordelen aard/ernst incident & verslag brengen aan rest van het bestuur

De bestuursverantwoordelijke (en eventuele andere hulp) onderzoeken het datalek om te zien of er daadwerkelijk sprake van een datalek is. Als het een datalek betreft, wordt er gekeken naar de informatie die gelekt is en de ernst van het datalek. De bestuursverantwoordelijke rapporteert de uitslag aan de rest van het bestuur. Bij de beoordeling spelen de volgende punten een rol:

- Is er sprake van verlies van persoonsgegevens; dit houdt in dat de studievereniging deze gegevens niet meer heeft, omdat deze zijn vernietigd of op een andere wijze verloren zijn gegaan;
- Is er sprake van onrechtmatige verwerking van persoonsgegevens; hieronder vallen de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens of verstrekking daarvan;
- Is er sprake van een enkele tekortkoming van kwetsbaarheid in de beveiliging;
- Kan er redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
- Zijn er persoonsgegevens van gevoelige aard gelekt;
  - Bijzondere persoonsgegevens conform artikel 9 AVG (artikel 16 Wbp);
  - Gegevens over de financiële of economische situatie van de betrokkene;

- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden gebruikt voor (identiteits)fraude;

Σ Leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen; betrek hierbij factoren als:

- De omvang van de verwerking; gaat het om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkene(n);
- De impact van verlies of onrechtmatige verwerking;
- Het delen van de persoonsgegevens binnen ketens; dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten kunnen optreden;
- Betrokkenheid van kwetsbare groepen; denk aan verstandelijk gehandicapten

3. Indien datalek; inlichten aangewezen instantie en onderzoek naar datalek

De aangewezen instantie van de Radboud Universiteit wordt op de hoogte gesteld waarmee op basis daarvan plannen worden gemaakt. Daarbij wordt onderzocht hoe het datalek zich heeft kunnen voordoen indien dit nog niet bekend was. In 2018 was de facultaire privacy manager van het FNWI Bjorn Bellink, het hoofd van C&CZ. Er kan contact worden opgenomen omtrent privacy via dpm@science.ru.nl (FNWI) en privacy@ru.nl (centraal).

4. Vaststellen datalek

Na overleg met de instantie van de Radboud Universiteit, wordt onderzoek naar het datalek afgerond en denkt het gehele bestuur na over vervolgplannen omtrent dit incident.

5. Rapporteren aan betrokkene(n)

Het bestuur neemt de afweging of betrokkene(n) ingelicht moeten worden over het datalek. Indien dit het geval is, neemt de bestuursverantwoordelijke contact met hen op. Of betrokkene(n) ingelicht dienen te worden, hangt af van de volgende punten:

Σ Indien de vereniging passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven (artikel 34a, lid 6, Wbp). Bij twijfel hierover dient het datalek gemeld te worden.

Σ Het datalek moet aan betrokkene(n) worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34, lid 2, Wbp).

Σ De melding aan betrokkene(n) mag achterwege blijven, als daarvoor zwaarwegende reden aanwezig zijn (artikel 43, Wbp). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in dit artikel. Op grond van artikel 43, onder e, Wbp mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

6. Verbeteringsmaatregelen bedenken en implementeren

Naar aanleiding van het datalek stelt het bestuur verbeteringsmaatregelen op om een soortgelijke situatie te voorkomen. Deze worden dan ook z.s.m. ingevoerd waarbij ook alle andere mogelijke datalekken worden onderzocht en verholpen.

7. Einde

Daarmee wordt het proces rondom datalekken afgesloten. Indien er weer een (mogelijk) datalek zich voordoet, dan wordt het proces weer in gang gezet.