Datalekprotocol

Wanneer er sprake is van een (mogelijk) datalek, kunnen de volgende stappen ondernomen worden.

1. **Identificeren mogelijk datalek**

Indien een (mogelijk) datalek wordt geconstateerd, wordt (de rest van) het bestuur ingelicht.

2. **Beoordelen aard en ernst van het incident**

Het bestuur onderzoekt het mogelijke datalek om te zien of er daadwerkelijk sprake is van een datalek. Als het een datalek betreft, wordt er gekeken naar de informatie die gelekt is en de ernst van het datalek. Bij de beoordeling spelen de volgende punten een rol:

- Is er sprake van verlies van persoonsgegevens? Dit houdt in dat de vereniging 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 onbevoegde toegang tot verwerkte persoonsgegevens of verstrekking daarvan.
- Is er sprake van tekortkomingen of 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? Denk aan onder andere:
    - Bijzondere persoonsgegevens conform artikel 16 Wet Bescherming Persoonsgegevens (WBP);
    - Gegevens over de financiële of economische situatie van de betrokkene;
    - Gegevens die kunnen leiden tot bevooroordeling of uitsluiting van de betrokkene;
    - Gebruikersnamen, wachtwoorden en/of andere inloggegevens;
    - Gegevens die kunnen worden gebruikt voor (identiteits)fraude.
- 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 betrokkenen?;
    - 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 bijvoorbeeld aan verstandelijk gehandicapten.

3. **Indien datalek van ernstige aard: inlichten Autoriteit Persoonsgegevens**

Indien het datalek van ernstige aard is, kan het verplicht zijn om het datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Is dit het geval, dan wordt de AP op de hoogte gesteld. Op basis daarvan worden plannen gemaakt om het lek te dichten en betrokkenen te informeren. Daarbij wordt onderzocht hoe het datalek zich heeft kunnen voordoen indien dit nog niet bekend was.

4. **Rapporteren aan betrokkenen**

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

- Indien de vereniging passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkenen achterwege blijven (artikel 34a, lid 6, WBP). Bij twijfel hierover dient het datalek gemeld te worden.
- Het datalek moet aan de betrokkenen worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, lid 2, WBP).
- De melding aan de betrokkenen mag achterwege blijven, als daarvoor zwaarwegende redenen aanwezig zijn (artikel 43, WBP). Daarbij geldt wel dat de melding aan de betrokkenen 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 betrokkenen worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkenen.

5. **Verbeteringsmaatregelen bedenken en implementeren**

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

Mogelijke verbetermaatregelen om een datalek te voorkomen zijn onder andere:

- Het houden van een interne opschoonactie. Verwijder bijvoorbeeld e-mails of bestanden die niet meer nodig zijn en schoon adresboeken op: hier zitten namelijk vaak persoonsgegevens in. Hiermee wordt voorkomen dat een datalek onnodig veel persoonsgegevens raakt. Verwijder persoonsgegevens en controleer of deze gegevens nog in een back-up zitten. Zo ja, verwijder de gegevens dan ook uit de back-up.
- Het instellen van “versturen in bcc” als standaardoptie in e-mailprogramma’s. Hiermee wordt de kans op een datalek verkleind door per ongeluk de e-mailadressen van een groepsmail zichtbaar te maken voor iedereen.
- Er voor zorgen dat persoonsgegevens alleen ingezien kunnen worden door daarvoor bevoegde personen. Houd goed in de gaten wie persoonsgegevens in kunnen zien en controleer periodiek op onrechtmatige inzage.
- Het regelmatig veranderen van wachtwoorden. Sla de wachtwoorden op een veilige plek op, waar alleen de juiste personen er toegang tot hebben.

6. **Einde**

Daarmee wordt het proces rondom datalekken afgesloten. Elk datalek wordt opgenomen in het bijbehorende register. Indien zich weer een (mogelijk) datalek voordoet, wordt het proces opnieuw in gang gezet.

7. Meer informatie

Zie Datalek? Dit moet u doen | Autoriteit Persoonsgegevens voor meer informatie over wat te doen bij een datalek.

Dit document is voor het laatst bijgewerkt op 12-08-2026