PROCEDURE DATALEK

ECODASS INSURANCE SERVICES

STAP 1 INTERN MELDEN BEVEILIGINGSINCIDENT

Meld ieder vermoeden van een datalek zo spoedig mogelijk en uiterlijk binnen 24 uur bij de compliance officer. Bij afwezigheid van de compliance officer kan deze melding gedaan worden bij de directie.

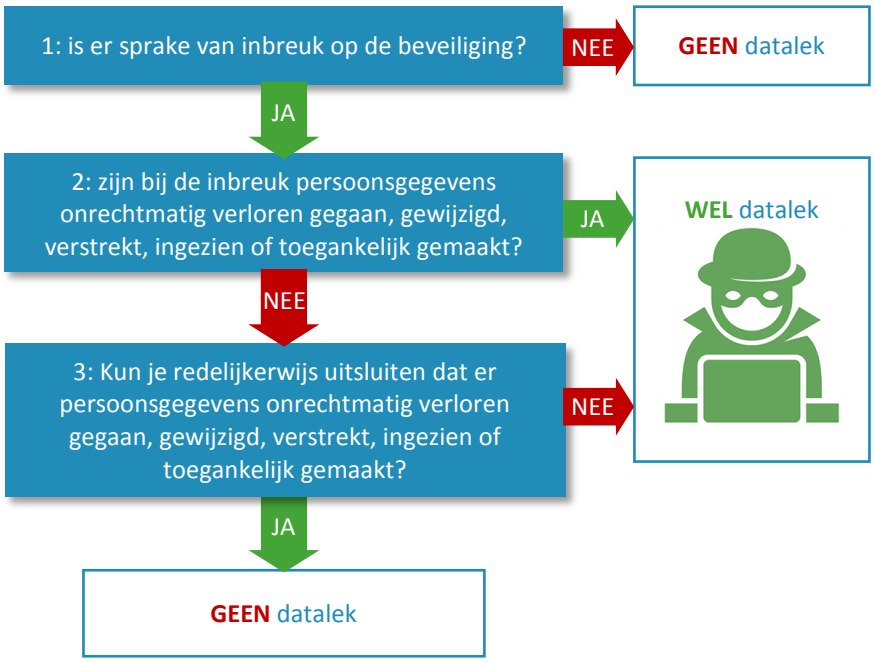
Door: alle medewerkers

BEVEILIGINGSINCIDENT MET PERSOONSGEGEVENS: Intern melden.

STAP 2 BEPALEN OF SPRAKE IS VAN EEN DATALEK

Een datalek is een inbreuk op de beveiliging waarbij persoonsgegevens (per ongeluk of opzettelijk) verloren zijn gegaan, ongeoorloofd zijn gewijzigd, verstrekt, ingezien of toegankelijk zijn gemaakt

Beoordeel bij ieder mogelijk lek direct of sprake is van een datalek.



Door: compliance officer

BEPALEN WEL/GEEN DATALEK: Beveiligingsincident + mogelijk inbreuk of verlies persoonsgegevens.

STAP 3 REGISTREREN DATALEK

Onderzoek aard en ernst van het incident en beoordeel welke maatregelen getroffen moeten worden om schade te beperken en herhaling te voorkomen.

Registreer, al dan niet gefaseerd, de volgende feiten zodra deze bekend zijn:

1. Feiten over het lek:
   - een korte omschrijving van het lek;
   - wanneer het plaatsvond;
   - wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd?);

REGISTREREN DATALEK: Onderzoeken, maatregelen treffen en registreren

- van welke groep(en) personen er gegevens gelekt zijn, en om hoeveel personen het gaat;
- om welke soorten gegevens het gaat.

2. de (mogelijke) gevolgen van de inbreuk (bijvoorbeeld een risico op identiteitsfraude of reputatieschade);
3. de maatregelen die zijn genomen naar aanleiding van het lek.
   - Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken?
   - Welke actie is ondernomen om risico op herhaling te voorkomen of zoveel mogelijk te beperken?

Door: Compliance officer

STAP 4 BEPALEN OF DATALEK GEMELD MOET WORDEN AAN AUTORITEIT PERSOONSGEGEVENS EN/OF AFM

MELDING TOEZICHTHOUDERS NODIG? Persoonsgegevens van gevoelige aard, aard & omvang van inbreuk, Wft-incident

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als de kans aanzienlijk is op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Beoordeel bij ieder datalek of het gemeld moet worden aan de Autoriteit Persoonsgegevens

1) Zijn de gelekte persoonsgegevens van gevoelige aard:
   a. Bijzondere persoonsgegevens
      - Gezondheidsgegevens
   b. Andere persoonsgegevens van gevoelige aard
      - Strafrechtelijke persoonsgegevens
      - Gegevens over financiële of economische situatie
      - Inloggegevens zoals gebruikersnamen en wachtwoorden
      - Gegevens die kunnen worden misbruikt voor (identiteits)fraude
2) Kan de aard en omvang leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen:
   a. Gaat het om veel gegevens per persoon
   b. Gaat het om gegevens van grote groepen personen
   c. Gaat het om gegevens van kwetsbare groepen personen
   d. Zijn de beslissingen die o.b.v. de gegevens worden genomen ingrijpend
   e. Worden de gegevens met andere partijen gedeeld?

Beoordeel ook bij ieder datalek of het gemeld moet worden aan de AFM
Is sprake van een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van de onderneming, meldt het dan als Wft-incident aan de AFM. Raadpleeg de incidentenregeling.

Door: Compliance officer

STAP 5 MELDING MAKEN EN REGISTRATIE BIJWERKEN

MELDING MAKEN: Autoriteit Persoons-gegevens en AFM en bijwerken interne registratie

1. Meld het datalek zo snel mogelijk aan de Autoriteit Persoonsgegevens, zo mogelijk uiterlijk binnen 72 uur nadat het lek bekend werd. Als nog niet alle kennis over het lek bekend is, doe dan alvast een incomplete melding bij de toezichthouder dat er een lek heeft plaatsgevonden. Verstrek de overige verplicht te verstrekken zodra deze bekend is (gefaseerd) aan de toezichthouder.
   https://datalekken.autoriteitpersoonsgegevens.nl/

2. Werk de interne registratie bij met een overzicht van de melding

Door: Compliance officer

3. Meld het datalek aan de AFM (raadpleeg de incidentenregeling)
https://www.afm.nl/nl-nl/professionals/onderwerpen/misstanden-incidenten
Door: Compliance officer, zie incidentenregeling

STAP 6 MAATREGELEN TREFFEN

1. Neem de noodzakelijke maatregelen naar aanleiding van het datalek:
   - om schade te voorkomen of zoveel mogelijk te beperken (bijvoorbeeld het op afstand wissen van gegevens, of het wijzigen van wachtwoorden)
   - om te zorgen dat het niet nog een keer kan gebeuren

Door: Compliance officer en Team ICT

MAATREGELEN:
schade beperken en herhaling voorkomen

STAP 7 BEPALEN OF DATALEK GEMELD MOET WORDEN AAN BETROKKENE(N)

1. Beoordeel bij ieder datalek of het gemeld moet worden aan de Betrokkene(n)
   - Melding aan de Betrokkene(n) is niet verplicht op grond van de AVG voor een financiële onderneming met een Wft-vergunning
   - Melding aan de Betrokkene(n) kan wel volgen uit de eigen verantwoordelijkheid richting de klant (zorgplicht).
2. Meld indien nodig het datalek rechtstreeks aan de Betrokkene(n)

Door: Compliance officer, zie incidentenregeling

MELDING BETROKKENE(N):
alleen op grond van zorgplicht

STAP 8 BEPALEN OF DATALEK GEMELD MOET WORDEN AAN POLITIE

1. Beoordeel bij ieder datalek of er aanwijzingen voor of vermoedens van strafbaar handelen bestaan (zoals hacken)
2. Doe indien nodig aangifte bij de politie

Door: Compliance officer, zie incidentenregeling

MELDING POLITIE:
bij verdenking strafbaar handelen

STAP 9 AFRONDEN MELDING EN BIJWERKEN REGISTRATIE

1. Werk de melding aan Autoriteit Persoonsgegevens bij zodat deze volledig en actueel is (zie stap 5) en daarmee afgerond is
2. Werk de eigen registratie bij zodat deze volledig en actueel is (zie stap 3)
3. Sluit het dossier en bewaar gedurende minimaal één jaar of zoveel langer als nodig

Door: Compliance officer

AFRONDEN:
bijwerken registratie

ECODASS
INSURANCE SERVICES