Protocol Meldplicht Datalekken

De Commercieele Club Groningen

Inleiding

Wanneer er een datalek heeft plaatsgevonden is De Commercieele Club, hierna de CCG, als verwerkingsverantwoordelijke verplicht dit binnen 72 uur te melden aan de Autoriteit Persoonsgegevens. Het doel van de meldplicht is om de schade voor betrokkenen als gevolg van een datalek zo minimaal mogelijk te houden. Dit protocol beschrijft welke procedure gevolgd wordt bij een melding datalek.

Beveiligingsincidenten melden aan de CCG

Hierna wordt uitgelegd dat er een verschil is tussen een zwakke plek in de beveiliging, een beveiligingsincident en een datalek. Het is voor de CCG belangrijk om in voorkomende gevallen tijdig te kunnen beoordelen of er sprake is van een datalek. Daarom worden verwerkers, leden van de CCG, secretariaat en bestuur verzocht om – ook bij twijfel – incidenten te melden via privacyloket@commercieeleclubgroningen.nl.

Wat is een datalek?

Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan, waarbij persoonsgegevens verloren zijn gegaan, of wanneer niet is uit te sluiten dat de persoonsgegevens onrechtmatig verwerkt worden.
Het gaat om situaties waarbij persoonsgegevens (mogelijk) zijn:

a) vernietigd of verloren,
b) gewijzigd,
c) verstrekt of toegankelijk gemaakt.

Niet iedere datalek is zo ernstig dat dit moet worden gemeld. Melding aan de Autoriteit Persoonsgegevens is verplicht als er sprake is van of kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Melding aan de betrokkenen is verplicht als er kans is op ongunstige gevolgen voor hun persoonlijke levenssfeer.
Een beveiligingsincident is geen datalek wanneer er geen persoonsgegevens mee gemoeid zijn. Soms is er ook sprake van een zwakke plek in de beveiliging; ook dat is geen datalek.

Voorbeelden van datalekken

Er is sprake van een datalek als de persoonsgegevens die de CCG verwerkt, mogelijk in handen komen van derden, die geen toegang tot deze informatie zouden mogen hebben. Voorbeelden zijn:

a) De server bij de IT-leverancier wordt gehackt en de informatie wordt gestolen.
b) Door een IT-incident ziin de persoonsgegevens verloren gegaan en er is geen complete en actuele reservekopie van de gegevens.
c) De computer in het secretariaat wordt gehackt of ingezien door derden.
d) Er is een mailing verstuurd met de adressen in een “cc-veld”.
e) Verlies of diefstal van een USB-stick, laptop, Ipad of smartphone met daarop persoonsgegevens.
f) Er wordt mail verstuurd naar een verkeerd mailadres.
g) Verlies of diefstal van een geprinte lijst met persoonsgegevens.
h) Wachtwoorden om in te loggen zijn in handen van een derde gevallen, waardoor deze onbevoegd toegang heeft tot persoonsgegevens.

Wat heeft de CCG geregeld in het kader van de Meldplicht Datalekken?

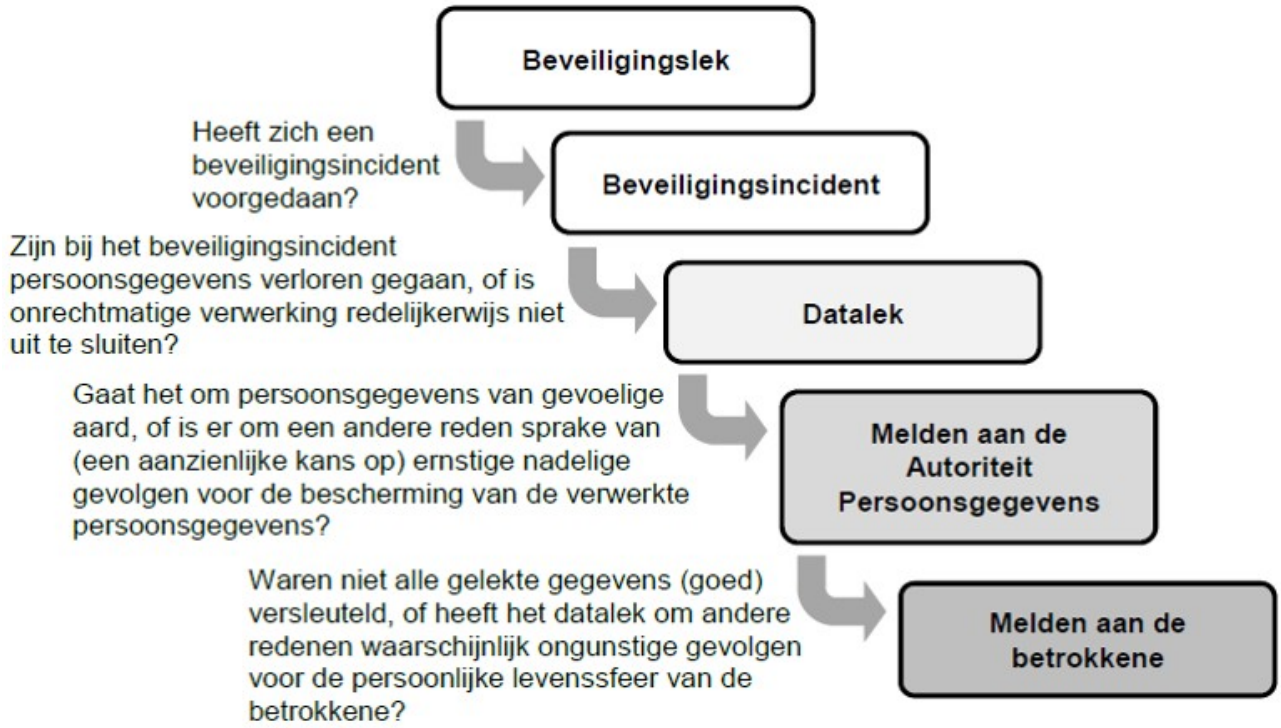
De CCG heeft verwerkersovereenkomsten afgesloten met haar verwerkers, waarin afspraken zijn opgenomen over passende maatregelen om datalekken te voorkomen en over het tijdig melden van een datalek, zodat de CCG aan haar verplichtingen als verwerkingsverantwoordelijke kan voldoen.
In de Privacyverklaring ten behoeve van leden wordt kort uitleg gegeven over datalekken en wordt uitgelegd hoe leden een datalek kunnen melden.
Datalekken kunnen gemeld worden via privacyloket@commercieeleclubgroningen.nl.
Binnenkomende mail op dit mailadres wordt dagelijks gecheckt door de secretaresse en/of de bestuurssecretaris van de CCG. Bij afwezigheid van beiden wordt vervanging geregeld. Al deze personen kunnen een datalek herkennen en naar bevind van zaken handelen, zodat de schade beperkt blijft.

Het vastleggen van de (veiligheids)incidenten

De CCG legt alle beveiligingsincidenten, waaronder datalekken vast in een incidentregistratie. Hierin wordt een korte omschrijving gegeven van:

a) het incident
b) de feiten, context en analyse
c) of het wel of niet een datalek is
d) de eventuele melding aan de Autoriteit Persoonsgegevens (AP)
e) de eventuele melding aan betrokkenen
f) de maatregelen

Beslisboom Melden Datalek



Procedure Melding Datalek

Stap 1: incidentmelding via privacyloket@commercieeleclubgroningen.nl.

Een (beveiligings)incident kan worden aangedragen door een lid, bestuurslid, een medewerker of een verwerker van de CCG. Maar ook op andere manieren kan een incident aan het licht komen, bijvoorbeeld door een klacht of een signaal uit de buitenwereld. Bijvoorbeeld naar aanleiding van een melding die direct bij de Autoriteit Persoonsgegevens is gedaan.

Stap 2: verzamelen feiten en analyse

De beheerders van het privacyloket beoordelen of dit een datalek is aan de hand van de volgende vragen:

1. Is er sprake van een inbreuk op de beveiliging?
2. Zijn bij de inbreuk persoonsgegevens verloren gegaan?
3. Kan ik redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt?

Om te bepalen of er sprake is van een echt datalek en een voorlopige inschatting te maken van de ernst, verzamelen en analyseren de beheerders van het privacyloket de feiten en omstandigheden waaronder het incident plaatsvond.

De beheerders van het privacyloket overleggen met de (vice)voorzitter van het bestuur van de CCG. Vervolgens wordt door de (vice)voorzitter vastgesteld of de melding al dan niet een datalek is.

Stap 3a: de melding is geen datalek

De beheerders van het privacyloket registreren de melding in de incidentregistratie voor intern gebruik (t.b.v. het signaleren van trends en leerpunten). De melder krijgt een reactie terug.

Stap 3b: de melding is een datalek

De beheerders van het privacyloket zorgen ervoor dat er zo snel mogelijk maatregelen worden genomen om verder verlies van persoonsgegevens of schade aan persoonsgegevens te voorkomen.
Voorbeelden van maatregelen zijn:

a) Onmiddellijk contact opnemen met de IT-supplier bij bijvoorbeeld een malware- of virusbesmetting om te overleggen over mogelijke aanpassingen in de systemen.
b) Het wijzigen van een wachtwoord, zodat een derde geen toegang meer heeft.
c) Het waarschuwen van de leden, zodat zij zelf maatregelen kunnen nemen.
d) Het resetten van alle wachtwoorden, waarbij leden een nieuw wachtwoord moeten opgeven.
e) Andere partijen die betrokken zijn bij de dienstverlening van de CCG waarschuwen.

Stap 3c: beoordelen of melden aan de Autoriteit Persoonsgegevens verplicht is

De beheerders van het privacyloket beoordelen of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens aan de hand van de volgende vragen:

1. Zijn er persoonsgegevens van gevoelige aard gelekt?
2. Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

De beheerders van het privacyloket delen de bevindingen met de (vice)voorzitter van het bestuur van de CCG. Vervolgens wordt door de (vice)voorzitter vastgesteld of de melding al dan niet gemeld moet worden aan de Autoriteit Persoonsgegevens.

Stap 4: het datalek melden aan de Autoriteit Persoonsgegevens

De beheerders van het privacyloket dienen het datelek onverwijld te melden aan de Autoriteit Persoonsgegevens. Dit moet zonder onnodige vertraging en binnen 72 uur na de ontdekking gebeuren.

Als er nog niet volledig zicht is op wat er is gebeurd en om welke persoonsgegevens het gaat, doen de beheerders van het privacyloket de melding op basis van de gegevens die op dat moment beschikbaar zijn. De melding kan naderhand aangevuld of ingetrokken worden.

De melding wordt gedaan met het formulier “Melden Datalekken bij Autoriteit Persoonsgegevens” op de website van de AP. Bij de melding moet in ieder geval worden aangegeven:

a) De aard van de inbreuk.
b) De instanties waar meer informatie over de inbreuk kan worden verkregen.
c) Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk en maatregelen die de CCG heeft getroffen om deze gevolgen te beperken.

De beheerders van het privacyloket registreren de melding in de incidentregistratie. De melder krijgt een reactie terug.

Stap 5: bepalen of het datalek gemeld moet worden aan de betrokkenen

Melding aan de AP betekent niet automatisch dat het datalek ook gemeld moet worden aan de betrokkene.

De beheerders van het privacyloket maken hiervoor een aparte afweging aan de hand van de volgende vragen:

1. Zijn er persoonsgegevens van gevoelige aard gelekt?
2. Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?
3. Zouden betrokkenen kunnen worden geschaad door bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie?

De beheerders van het privacyloket delen de bevindingen met de (vice)voorzitter van het bestuur van de CCG. Vervolgens wordt door de (vice)voorzitter vastgesteld of de melding al dan niet gemeld moet worden aan de betrokkenen.

NB.
Een inbreuk op de ledenadministratie van de CCG kan leiden tot het mogelijke ongemak voor de vereniging en de leden, maar een melding aan de AP zal niet snel aan de orde zijn, omdat de CCG geen persoonsgegevens van gevoelige aard verwerkt.

Stap 6: melden aan de betrokkene

De beheerders van het privacyloket en (vice)voorzitter beoordelen of er een melding aan betrokkene moet worden gedaan. Hierbij worden een aantal aspecten afgewogen:

a) Bieden cryptografie of andere technische beschermingsmaatregelen voldoende bescherming?
b) Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van betrokkene?
c) Zijn er zwaarwegende redenen om de melding aan betrokkene achterwege te laten?

In voorkomend geval stuurt de CCG een e-mail naar betrokkene(n), waarin wordt aangegeven:

a) wat er gebeurd is (de aard van de inbreuk)
b) welke maatregelen de CCG heeft getroffen
c) hoe betrokkene zelf eventuele negatieve gevolgen tegen kan gaan
d) hoe betrokkene de CCG kan bereiken voor vragen

De beheerders van het privacyloket registreren de melding in de incidentregistratie.

NB.
Een inbreuk op de ledenadministratie van de CCG kan leiden tot het mogelijke ongemak voor de vereniging en de leden, maar een melding aan betrokkene(n) zal niet snel aan de orde zijn, omdat de CCG geen persoonsgegevens van gevoelige aard verwerkt.