Definitieve versie juni 2024

Protocol datalekken

rentree. thuis in Deventer

Procedure:

BO besluit d.d. 27-06-2024

Inleiding
Een informatiebeveiligingsincident of datalek is elke onverwachte of onverhoopte gebeurtenis die de informatieveiligheid van de gegevens kan aantasten. Binnen Rentree onderscheiden we drie soorten informatiebeveiligingsincidenten:

1. Een ICT incident: bijvoorbeeld malware, phishing, onverwachte werking van software of apparaat waarbij gegevens verloren dan wel niet beschadigd raken. Tevens onjuiste rechten hebben/opmerken in een informatiesysteem is een ICT incident.
2. Een datalek: een datalek is een beveiliginginsincident waarbij (mogelijk) persoonsgegevens of gevoelige informatie kan zijn verloren of uitgelekt. Bijvoorbeeld bij het verliezen van een USB stick, een gestolen laptop, het kwijtraken of verkeerd bezorgen van een fysieke brief/mail. Meld datalekken binnen 24 via Jira
3. Overige incidenten: indien je verdachte telefoontjes krijgt of personen die trachten informatie van je te bemachtigen buiten het kantoor.

Alle informatiebeveiligingsincidenten worden door de ICT manager behandeld. Deze bepaalt of het noodzakelijk is om de eventuele betrokkene op de hoogte te stellen van een datalek en/of een melding gedaan dient te worden aan de Autoriteit Persoonsgegevens. De melding kan mogelijke gevolgschade voorkomen of beperken. Ook helpt je melding altijd bij een verdere verbetering van de informatiebeveiliging, meld daarom altijd!

Wat betekent de meldplicht?
Een datalek kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van betrokkenen doordat de weggelekte gegevens oneigenlijk gebruikt kunnen worden. Identiteitsfraude is hiervan een voorbeeld maar ook kan gedacht worden aan ongewenste profilering of doorbreking van bewust gekozen anonimiteit. Om ernstige nadelige consequenties voor de bescherming van persoonsgegevens te beperken is een meldplicht ingevoerd bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens.

De meldplicht houdt in dat de verantwoordelijke een datalek moet melden bij de Autoriteit Persoonsgegevens. Altijd? Nee. Of een datalek gemeld moet worden, is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen.

Daarnaast moet degene die het betreft – de betrokkene- soms geïnformeerd worden. Niet alle datalekken hoeven gemeld te worden aan een betrokkene. Rentree hoeft de betrokkenen (de personen van wie Rentree gegevens verwerkt) alleen te informeren als een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert. Kunt u aannemelijk maken dat dit niet zo is? Dan hoeft Rentree het datalek niet aan de betrokkenen te melden. Om te bepalen of een datalek een hoog risico oplevert voor de betrokkenen, moet Rentree onder andere kijken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade. Het kan voorkomen dat een melding wel bij AP gedaan moet worden maar niet aan de betrokkene.

Een melding zal ‘onverwijld’ moeten worden gedaan. Het onverwijld melden houdt in dat men na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden van het datalek begint te lopen op het moment dat Rentree zelf, of een verwerker die Rentree heeft ingeschakeld, op de hoogte raakt van een incident waarbij persoonsgegevens kunnen zijn blootgesteld aan verlies of onrechtmatige verwerking. Uiterlijk binnen 72 uur na de ontdekking van het incident moet een melding bij de Autoriteit Persoonsgegevens binnen zijn, tenzij op dat moment inmiddels al uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt.

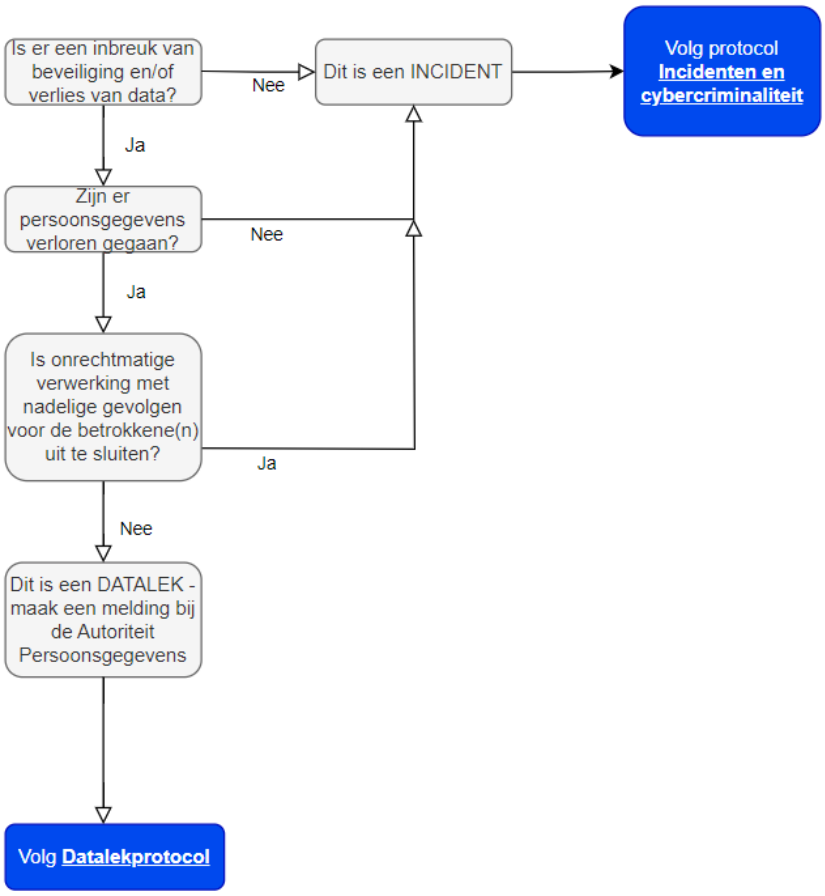
Wanneer is de meldplicht datalekken van toepassing?
De meldplicht geldt voor iedere verantwoordelijke voor de verwerking van persoonsgegevens (niet de verwerker). De wet verplicht, op een enkele uitzondering na, de verantwoordelijke tot melding van een datalek aan de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan de betrokkenen. Dit laatste is afhankelijk van de ernst van de zaak en de gevolgen voor de betrokkenen.

Om te beoordelen of een datalek gemeld moet worden, moeten alle van de volgende drie vragen bevestigend beantwoord worden:

- Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
- Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
- Heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de privacy van de betrokkenen.

Als er geen sprake is van verwerking van persoonsgegevens, dan is de meldplicht datalekken niet van toepassing.

Is dit een incident/datalek?
Een datalek is een beveiligingsincident waarbij persoonsgegevens betrokken zijn. Twijfel je of een incident een datalek is? Kijk dan naar de volgende flowchart:



Voorbeelden zijn:

- Een kwijtgeraakte USB-stick
- Een gestolen laptop
- Een inbraak door een hacker
- Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden
- Een mail verzonden aan een verkeerde ontvanger

Bij een inbreuk zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene, waartegen de beveiligingsmaatregelen bescherming moesten bieden.

Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Dit betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische maatregelen heeft genomen.

Hoe en wanneer meld ik een incident binnen Rentree
Iedereen is verplicht om als ontdekker van een (mogelijk) datalek het (mogelijk) incident te melden.

In de melding moet minimaal de volgende informatie worden gegeven:

- datum van de inbreuk
- samenvatting van het incident
- welk type gegevens het betreft
- mogelijke gevolgen voor Rentree als wel voor de betrokkene
- getroffen maatregelen (om de inbreuk aan te pakken en verdere uitbreiding te voorkomen)
- de aard van de datalek, d.w.z. beschrijving van de datalek. Welke informatie is weggevloeid?
- gegevens van de persoon waar meer informatie over het datalek kan worden verkregen

Vervolgens zal de ICT manager in overleg met de melder een afweging maken van het al dan niet melden aan de Autoriteit Persoonsgegevens en / of betrokkenen. De ICT manager zal conform wetgeving binnen 72 uur na ontdekking van het datalek melding maken aan de Autoriteit Persoonsgegevens.

Indien het datalek van een dusdanig grote omvang is met een grote impact voor Rentree dan wordt opschaling ingezet naar het bestuur van Rentree. Het bestuur bepaald te vervolg stappen in overleg met de ICT manager.

Wanneer moet Rentree een datalek melden aan de Autoriteit Persoonsgegevens?
Een datalek moet gemeld worden bij AP als er spraken is (potentiële) impact op de levensfeer van de betrokkenen. Een datalek brengt een hoog risico met zich mee wanneer het kan leiden tot lichamelijk, materiële of immateriële schade. Van een hoog risico is sprake als een datalek kan leiden tot:

1. Discriminatie
2. Identiteitsdiefstal
3. Financiële verliezen
4. Reputatieschade
5. Doorbreking van het beroepsgeheim
6. Ongeoorloofd ongedaan maken van gespeudonimiseerde gegevens
7. Een aanzienlijk economisch of maatschappelijk nadeel
8. Een situatie waarbij de betrokken hun rechten en vrijheden niet kunnen uitoefenen.
9. Als er sprake is van een datalek met bijzondere persoonsgegevens
10. Als er sprake is van een datalek met strafrechtelijke persoonsgegevens

11. Als er sprake is van een datalek over persoonlijke aspecten, bedoeld om profielen op te stellen of te gebruiken
12. Als er sprake is van een datalek met persoonsgegevens van kwetsbare groepen
13. Als er sprake is van een datalek met grote hoeveelheid persoonsgegevens en met gevolgen voor een hele grote groep mensen

Echter hoeft er geen melding gemaakt te worden als er persoonsgegevens gelekt zijn aan een betrouwbare partij. Betrouwbaar houdt in dat u er redelijk zeker van kunt zijn dat de onjuiste ontvanger geen kwaad in de zin heeft en dat de ontvanger niets doet met de per ongeluk ontvangen gegevens. Voorbeelden van betrouwbare ontvangers zijn:

- Partijen met wie Rentree een zakelijke relatie heeft, bijvoorbeeld een vaste leverancier
- Partijen die een wettelijk beroepsgeheim hebben, zoals een huisarts of een andere zorgverlener.

Een datalek die niet gemeld wordt aan de Autoriteit Persoonsgegevens dient wel altijd intern gerapporteerd te worden in het datalekken register.

Wanneer moet Rentree een datalek melden aan de getroffen persoon (betrokkene)?
Een datalek moet gemeld worden bij de betrokkene als er sprake is van hoog risico voor hun rechten en vrijheden. Om te bepalen of een datalek een hoog risico oplevert voor de betrokkenen, moet worden bekeken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Van een hoog risico is sprake als een datalek kan leiden tot:

1. Discriminatie
2. Identiteitsdiefstal
3. Financiële verliezen
4. Reputatieschade

Bij een melding aan de betrokkenen dient in ieder geval antwoord gegeven te worden op onderstaande vragen:

- Zijn de gegevens in handen gekomen van een onbevoegde? Of zijn de persoonsgegevens tijdelijk of permanent ontoegankelijk of verloren geraakt?
- Waren de persoonsgegevens onjuist of onvolledig? Of een combinatie?
- Om welke gegevens ging het? Wat is er met deze gegevens gebeurd?
- Zijn de gegevens in handen gekomen van een onbevoegde? Of zijn de persoonsgegevens tijdelijk of permanent ontoegankelijk of verloren geraakt?
- Waren de persoonsgegevens onjuist of onvolledig? Of een combinatie?
- Om welke gegevens ging het? Wat is er met deze gegevens gebeurd?
- Welke maatregelen stelt u voor of heeft u al getroffen?
- Kan de getroffen betrokkene zelf iets ondernemen
- Waar kunnen betrokkene met vragen terecht.

Begrippenlijst

Betrokkenen	Onder de Algemene Verordening Gegevensbescherming (AVG) worden "betrokkenen" individuen genoemd wiens persoonsgegevens worden verwerkt. Dit omvat elke levende persoon waarvan de gegevens worden verzameld en verwerkt, zoals klanten, werknemers, of websitegebruikers.
Autoriteit Persoonsgegevens	De Autoriteit Persoonsgegevens (AP) is in Nederland de toezichthoudende autoriteit op het gebied van gegevensbescherming. Deze instantie houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en andere privacywetten

Functionaris Gegevensbeschermer	Een functionaris voor gegevensbescherming (FG) is een functionaris binnen een organisatie die toezicht houdt op de naleving van de privacywetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). De FG adviseert en controleert de organisatie op het gebied van gegevensbescherming, en fungeert als contactpunt voor vragen en zorgen met betrekking tot privacy. Door het kleine formaat van Rentree heeft de ICT manager op dit moment deze verantwoordelijkheden.
Gepseudonimiseerde gegevens	Gepseudonimiseerde gegevens zijn persoonlijke gegevens waarbij directe identificerende informatie is vervangen door een pseudoniem, zoals een code of sleutel. Hoewel de gegevens nog steeds aan een specifieke persoon kunnen worden gekoppeld, vereist het extra informatie of sleutels om de identiteit te onthullen.
Geanonimiseerde gegevens	Geanonimiseerde gegevens zijn persoonlijke gegevens die zodanig zijn verwerkt dat ze niet langer kunnen worden gekoppeld aan een specifieke persoon. Door identificerende informatie te verwijderen of te wijzigen, wordt het praktisch onmogelijk om de oorspronkelijke persoon achter de gegevens te identificeren.

Juridisch kader
De Algemene Verordening Gegevensbescherming (AVG), ook bekend als de General Data Protection Regulation (GDPR), is een Europese wet die op 25 mei 2018 van kracht is gegaan. De AVG is ontworpen om de privacyrechten van individuen te versterken en de manier waarop organisaties persoonsgegevens verwerken te harmoniseren binnen de Europese Unie.

De AVG is bedoeld om de privacy van individuen te beschermen in het digitale tijdperk en om organisaties te stimuleren verantwoordelijk om te gaan met persoonsgegevens.
Dit document wordt jaarlijks geëvalueerd en/of bijgewerkt om te zorgen dat het protocol voor datalekmanagement effectief blijft en voldoet aan de eisen van de AVG.

Referenties
- Autoriteit persoonsgegevens
- AVG