Regio Gooi en Vechtstreek

MEMO

Handreiking beoordeling datalekken AVG

Algemeen	
Aan	CMT
Van	Anne Cnossen
Datum	27 september 2019
Verspreiden	Nee
Kenmerk	19.0013574

1. Inleiding

Vaak begint een datalek als vermoeden van een datalek of een 'informatieveiligheidsincident'. Zo'n vermoeden of incident is daadwerkelijk een datalek indien sprake is van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.

De Europese toezichhouders hebben Richtsnoeren opgesteld die de verwerkingsverantwoordelijke ondersteunen bij de beoordeling of een mogelijk datalek daadwerkelijk een datalek is en of aan de AP (en betrokkene) moet worden gemeld. Deze Richtsnoeren dienen tevens als uitgangspunt voor de AP bij het toepassen van handhavende maatregelen.

Ten behoeve van het Team Privacyincidenten is een handzame en praktische handreiking gemaakt van de vragen die in het kader van de beoordeling van een mogelijk datalek nagelopen en beantwoord moeten worden. Deze handreiking is opgesteld aan de hand van de hiervoor genoemde Richtsnoeren en informatie van de Autoriteit Persoonsgegevens.

2. Definities en omschrijvingen

Er is sprake van een datalek als er bij een informatieveiligheidsincident toegang tót of vernietiging, wijziging of vrijkomen ván persoonsgegevens heeft plaatsgevonden zonder dat dit de bedoeling is. Een datalek moet ruim worden opgevat. Het gaat om voorvallen waarbij de bescherming van persoonsgegevens is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies, onrechtmatige inzage of onrechtmatige verwerking. Voorbeelden van datalekken zijn:

- kwijtraken van een brief met persoonsgegevens bij de post
- verzenden van persoonsgegevens naar een verkeerd e-mailadres
- versturen/beschikbaar stellen via een portal van te veel (onnodige) gegevens aan derden
- kwijtraken van een onbeveiligde USB-stick met persoonsgegevens
- diefstal van een laptop, iPad e.d. met persoonsgegevens
- een malware besmetting
- verzenden van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (CC i.p.v. BCC)

Overige definities relevant in het kader van de beoordeling van datalekken zijn:

- betrokkene: degene op wie een persoonsgegeven betrekking heeft.
- inbreuk op de beveiliging/informatieveiligheidsincident: inbreuk op de passende technische en organisatorische maatregelen die moeten worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen.
- datalek/privacyincident: een informatieveiligheidsincident waarbij persoonsgegevens vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk gemaakt.

- persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- bijzondere persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt en genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, gegevens over gezondheid en gegegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
- verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval de Regio.
- verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

3. Te beantwoorden vragen

De vier belangrijkste vragen om een datalek en de te nemen stappen te kunnen beoordelen zijn:

- of er sprake is geweest van een datalek,
- wat er dan precies is gebeurd,
- of een melding gedaan moet worden aan de AP en
- of betrokkene(n) geïnformeerd moeten worden

In het navolgende wordt voor deze vragen aan de hand van de Richtsnoeren en informatie van de Autoriteit Persoonsgegevens een handreiking gegeven.

Stap 1) Is er sprake van een datalek?

Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (art. 4 AVG). Persoonsgegevens komen waar ze niet behoren te zijn. Ook als redelijkerwijs niet kan worden uitgesloten dat dit gebeurd is, is sprake van een datalek.

Inbreuk op de beveiliging?
Er moet sprake zijn geweest van een daadwerkelijke inbreuk op de beveiliging. Hiermee wordt gedoeld op inbreuk op de (in artikel 32 AVG vereiste) passende technische en organisatorische maatregelen die moeten worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Enkel een tekortkoming of zwakke plek in de beveiliging is nog geen inbreuk op de beveiliging. De eventueel getroffen beveiligingsmaatregelen moet onvoldoende zijn gebleken. Voorbeelden zijn de zoek geraakte USB-stick, gestolen laptop, een mail die naar een verkeerd mailadres wordt gestuurd of een calamiteit zoals brand in een datacentrum. Binnen de Regio spreken we in plaats van over een inbreuk op de beveiliging, over een informatieveiligheidsincident.

Als vast staat dat sprake is van een informatieveiligheidsincident moet gekeken worden of er (als gevolg van het incident) iets met de persoonsgegevens is gebeurd dat niet de bedoeling is.
Dat betekent dat er door het incident per ongeluk of op onrechtmatige wijze persoonsgegevens vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk gemaakt. Bij de Regio is het per ongeluk verstrekken of toegankelijk maken van persoonsgegevens het meest voorkomende scenario. De repressieve maatregelen en de herstelmaatregelen die getroffen zijn, zijn niet voldoende geweest om de gevolgen geheel weg te nemen.

Stap 2) Wat is er precies gebeurd?

Onderstaande vragen helpen om overzicht (wat is er precies gebeurd?) te krijgen op de situatie. Zodat de Regio de juiste vervolgstappen kan nemen. Deze vragen dienen behandeld te worden in het Team Privacyincidenten.

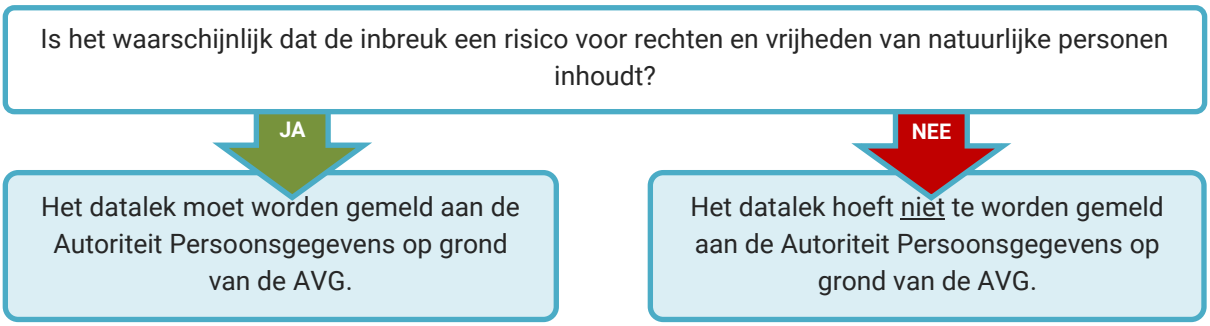
- Om wat voor soort datalek gaat het?
Er zijn drie categorieën datalekken te onderscheiden:
  - Inbreuk op de vertrouwelijkheid
Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
  - Inbreuk op de integriteit
Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
  - Inbreuk op de beschikbaarheid
Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van, toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen. Bij de Regio komt inbreuk op de vertrouwelijkheid echter veruit het meest voor.

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En bestaat het lek nog steeds?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn er gelekt? Bijvoorbeeld naam, adres, e-mailadressen, BSN en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijvoorbeeld werknemers, scholieren, patiënten, inwoners etc. Gaat het om kwetsbare groepen? Bijvoorbeeld kinderen, gehandicapten of bejaarden.
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Is er zicht op wie de onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?

- Heeft de Regio vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 3) Moeten we het datalek melden aan de AP?
Niet alle datalekken hoeven bij de Autoriteit Persoonsgegevens (AP) te worden gemeld. Er moet gemeld worden tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor rechten en vrijheden van natuurlijke personen. Wel moeten álle datalekken geregistreerd worden.



Voor de beoordeling van het risico kan rekening worden gehouden met de volgende factoren:

- De aard van de inbreuk
Zijn er persoonsgegevens gewist, gewijzigd of verstrekt? Voorbeeld: het verstrekken van medische persoonsgegevens aan een onbevoegde, heeft andere gevolgen dan wanneer deze gegevens verloren zijn gegaan.

- De aard, gevoeligheid en omvang van de persoonsgegevens
Hoe gevoeliger de gegevens, hoe groter het risico op schade. Houd ook rekening met persoonsgegevens die al (openbaar) beschikbaar zijn. Want juist een combinatie van gegevens kan de impact groter maken.

- Gemak waarmee personen kunnen worden geïdentificeerd
Kun je op basis van het datalek eenvoudig zien om wie het gaat?

- Ernst van gevolgen voor personen
De gevolgen van een datalek kunnen ernstig zijn. Vooral wanneer het datalek kan leiden tot bijvoorbeeld identiteitsdiefstal of reputatieschade. Het risico wordt kleiner wanneer de gegevens in handen zijn gekomen van een betrouwbare ontvanger die er niet op uit is om schade te veroorzaken.

- Bijzondere kenmerken van de persoon
Wanneer gegevens van kwetsbare personen betrokken zijn bij het datalek, kunnen zij een groter risico op schade lopen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen voor de meeste mensen beperkt zijn, maar dit ligt anders voor mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor betrokkenen zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

- Bijzondere kenmerken van de verwerkingsverantwoordelijke
De risico's bij een datalek van een organisatie met veel bijzondere persoonsgegevens (m.n. gezondheidsgegevens) zoals de Regio is, zullen groter zijn dan bij een datalek met een mailinglijst van een krant.

- Het aantal getroffen personen
Over het algemeen kan een datalek grotere gevolgen hebben naarmate er meer personen bij betrokken zijn. Een inbreuk kan echter zelfs voor één persoon ernstige gevolgen hebben.

Stap 4) Moeten we het datalek melden aan de betrokkene?

Het datalek moet gemeld worden aan de betrokkene wanneer het waarschijnlijk is dat het datalek een **hoog** risico voor rechten en vrijheden van natuurlijke personen inhoudt, tenzij er vooraf of achteraf voldoende maatregelen zijn toegepast of mededeling aan betrokkene onevenredige inspanning vergt. In het laatste geval is dan wel een openbare mededeling of soortgelijke maatregel nodig waardoor de betrokkene doeltreffend wordt geïnformeerd. Denk hierbij aan plaatsing op een regionale nieuwswebsite of in een regionale krant.

Een hoog risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Wanneer de inbreuk betrekking heeft op bijzondere persoonsgegevens moet dergelijke schade als waarschijnlijk worden beschouwd. Bijzondere persoonsgegevens zijn:

- persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt en
- genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, gegevens over gezondheid en gegegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voorbeelden van **lichamelijke, materiële of immateriële schade** zijn:

- Discriminatie
bijvoorbeeld bij een datalek met gegevens over ras, geloof of seksuele geaardheid.

- Identiteitsdiefstal of –fraude
bijvoorbeeld bij een datalek met complete paspoortkopieën. Of het BSN in combinatie met andere persoonsgegevens (zoals geboortedatum).

- Financiële verliezen
bijvoorbeeld bij een datalek met creditcardgegevens waardoor het risico bestaat dat iemand online bestellingen kan plaatsen op kosten van een ander.

- Reputatieschade
bijvoorbeeld bij een datalek met gegevens over problematische schulden, verslaving of prestaties op het werk.

4. Zwaarwegende redenen voor niet melden (artikel 41 UAVG)

De melding mag, na een zorgvuldige belangenafweging, achterwege blijven in het belang van:
a. de nationale veiligheid;
b. landsverdediging;
c. de openbare veiligheid;
d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
j. de inning van civielrechtelijke vorderingen.