Protocol datalekken WIJ 3.0

Versie 2.0; 25-5-2018

Protocol datalekken

Voorliggend protocol is een bijlage bij het privacyreglement. Dit reglement dient ertoe bij te dragen dat er geen datalekken in de organisatie ontstaan. Mochten die er onverhoopt toch ontstaan, dan is in dit document terug te lezen hoe met deze datalekken omgegaan moet worden door WIJ 3.0

Datalek en beveiligingslek

Er is een onderscheid tussen een datalek en een beveiligingslek. Er is sprake van een beveiligingslek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet bijvoorbeeld gedacht worden aan het kwijtraken van een USB-stick, diefstal van een laptop of een inbraak door een hacker. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens. Indien er sprake is van een beveiligingsincident dient de interne incidentmeldingsprocedure te worden gevolgd.

Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet uitgesloten kan worden. Intern moet ook een datalek meegenomen worden in de interne incidentmeldingsprocedure.

Melden aan de Autoriteit Persoonsgegevens

Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard kan gedacht worden aan:

1. Bijzondere persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
2. Gegevens over de financiële of economische situatie van de betrokkene, zoals (problematische) schulden, salaris- en betalingsgegevens.
3. Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, denk hierbij aan: gokverslaving, prestaties op school of werk of relatieproblemen.
4. Gebruikersnamen, wachtwoorden en andere inloggegevens
5. Gegevens die kunnen worden misbruikt voor (identiteits-)fraude, onder andere biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer

Een melding moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan **72 uur** na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar gesteld: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage).

Enkele voorbeelden van datalekken die moeten worden gemeld aan de Autoriteit Persoonsgegevens:

- Een medewerker van WIJ 3.0 verliest een USB of laptop met onversleutelde gegevens
- Door een beveiligingslek blijkt dat persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen) van werknemers door onbevoegden zijn ingezien

- Enkele personeelsleden maken gebruik van het wachtwoord van een ander persoon om toegang te krijgen tot persoonsgegevens. Er is op onrechtmatig wijze toegang verkregen tot persoonsgegevens. Bovendien is er sprake van een schending van interne voorschriften.

Constateer je een datalek, dan moet je dit melden aan je leidinggevende en tevens doorgeven aan Gerard de Punder.

Melden aan de betrokkene

Als geconcludeerd wordt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan betekent dat niet automatisch dat dit datalek ook gemeld dient te worden aan de betrokkene. Hiervoor dient een aparte afweging gemaakt te worden. Het bestuur van Wij 3.0 maakt deze afweging.

De wet geeft aan dat een melding gedaan moet worden aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Alleen als passende technische beschermingsmaatregelen zijn genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven.

Binnen welke termijn en hoe dient het datalek gemeld te worden aan de Autoriteit Persoonsgegevens?

Het datalek moet direct gemeld worden aan de Autoriteit Persoonsgegevens. Dat houdt in dat, na het ontdekken van een mogelijk datalek, enige tijd genomen mag worden voor nader onderzoek om een onnodige melding te voorkomen.

Zonder onnodige vertraging, en zo mogelijk binnen **72 uur** na de ontdekking, dient melding te worden gedaan bij de Autoriteit Persoonsgegevens, tenzij op dat moment intussen uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien het incident later dan 72 uur na ontdekking aan de toezichthouder wordt gemeld, dan kan desgevraagd gemotiveerd worden waarom de melding later is gedaan. Het is mogelijk dat na 72 uur na de ontdekking van het incident nog niet volledig inzichtelijk is wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt de melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog aangevuld of ingetrokken worden.

Na melding verstuurt de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging.

Binnen welke termijn en hoe moet het datalek gemeld worden aan de betrokkene?

Indien is gebleken dat het datalek aan betrokkene gemeld dient te worden, dient dit onverwijld te geschieden. Dit houdt in dat, na het ontdekken van het datalek, nog enige tijd genomen mag worden voor nader onderzoek. Hierbij moet wel rekening worden gehouden met het feit dat de betrokkene mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene wordt geïnformeerd, hoe eerder deze in actie kan komen.

In de melding aan de Autoriteit Persoonsgegevens moet aangeven worden of het datalek al aan de betrokkene is gemeld en, wanneer dit niet het geval is, wanneer dit alsnog gedaan zal worden.

Bij de kennisgeving aan de betrokkene dient in ieder geval vermeld te worden:

- Aard van de inbreuk
- Eventueel te treffen maatregelen die de betrokkene wordt aanbevolen om negatieve gevolgen van de inbreuk te beperken

Voorts wordt hierbij de contactgegevens opgenomen zodat de betrokkene terecht kan indien hij/zij vragen heeft over het datalek. Verder kan aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken.

Welke gegevens moeten worden vastgelegd?

WIJ 3.0 houdt een overzicht bij van alle datalekken die onder de meldplicht vallen. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen. **WIJ 3.0 bewaart deze data minimaal twee jaar, om:**

- Lering te trekken uit het datalek en de wijze waarop is gehandeld
- Antwoord te kunnen geven op vragen van betrokkenen en anderen
- Alsnog melden van het datalek aan betrokkenen te kunnen doen indien dit in eerste instantie achterwege is gelaten en de omstandigheden vereisen dat dit alsnog wordt gedaan
- Rekening te houden met het feit dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat indien dit aan de orde is, bewijsmateriaal verzameld moet worden.

Wat doet de Autoriteit Persoonsgegevens met de melding?

Na het melden van een datalek stuurt de Autoriteit Persoonsgegevens per omgaande een ontvangstbevestiging. Het is de verantwoordelijkheid van WIJ 3.0 om de oorzaak van het datalek op te sporen en om maatregelen te treffen om herhaling te voorkomen. De ontvangen datalekmeldingen stellen de Autoriteit Persoonsgegevens in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijk raken of waarvan zij last kunnen ondervinden. Als het datalek niet is gemeld aan de betrokkene en deze waarschijnlijk ongunstige gevolgen zal hebben voor de betrokkene, kan de Autoriteit verlangen dat alsnog een kennisgeving wordt gestuurd. Dit staat gelijk aan een **bindende aanwijzing**. Het niet nakomen kan voorts worden bestraft met een **bestuurlijke boete**. Deze bestuurlijke boete bedraagt maximaal **820.000 euro**.

Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een **bindende aanwijzing** opleggen voorafgaand aan eventuele oplegging van een **bestuurlijke boete**.

De Autoriteit Persoonsgegevens houdt een niet openbaar register bij van de ontvangen datalekmeldingen. De Autoriteit houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en kan derhalve onderzoek doen naar de mogelijke overtredingen van de wet. Hiervoor kan de Autoriteit gebruik maken van informatie uit de ontvangen datalekmeldingen.