

Bijlage 15: Afspraken betreffende Inbreuken Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden.

Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de Autoriteit Persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer.

Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, malware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum.

In deze Procedure Datalek wordt in meer detail uiteengezet hoe Opdrachtnemer in onverhoopt geval met het verlies van dergelijke persoonsgegevens omgaat.

Uitgangspunten

1. De Opdrachtnemer verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Opdrachtgever.
2. De Opdrachtnemer neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, zoals tevens staat beschreven in de tussen Opdrachtgever en Opdrachtnemer overeengekomen hoofdovereenkomst;

Direct melding doen bij de FG Opdrachtgever

3. De data lek melding moet Opdrachtnemer direct via email en telefonisch worden gedaan bij de Functionaris gegevensbeschermmer van de Opdrachtgever (kortweg FG) en schriftelijk worden vastgelegd.
4. Het telefoonnummer van de FG luidt 038 – 42 681 65
5. Het e-mail adres van de FG luidt jurist@skal.nl
6. De FG meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.
7. De FG krijgt van de Opdrachtnemer de volgende gegevens en legt deze gegevens ook vast:
 - naam van de melder;
 - de contactpersoon voor de melding;
 - datum en tijd van de melding;
 - aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
 - welke persoonsgegevens vallen onder de melding;
 - om welk aantal gegevensrecords gaat het;
 - welke (groepen) personen zijn betrokken bij de melding;
 - welke maatregelen zijn of worden door de melder getroffen;

- welke gevolgen zijn er volgens de melder voor de betrokkenen.

Escalatie bij afwezigheid

8. Bij afwezigheid van de FG wordt diens rol ingevuld door een waarnemer van Opdrachtgever. Buiten kantoor tijden en in het weekend wordt de melding door de Opdrachtnemer gedaan via jurist@skal.nl.
9. Opdrachtnemer is ervan op de hoogte dat een datalek door Opdrachtgever zo spoedig mogelijk, maar uiterlijk binnen 72 uur, gemeld moet worden bij de Autoriteit Persoonsgegevens.

Melding

10. Met het oog daarop zal Opdrachtnemer al het mogelijke doen om Opdrachtgever in staat te stellen deze melding tijdig en volledig te doen. Opdrachtnemer neemt in het geval van een datalek of een vermoeden daarvan zo spoedig contact op met de FG of diens plaatsvervanger van Opdrachtgever, ook indien nog niet alle relevante informatie bekend is.
11. Opdrachtnemer zal Opdrachtgever binnen 48 uur na constatering van het datalek voorzien van de benodigde gegevens voor het doen van de melding, zoals omschreven op het formulier bij het Meldloket Datalekken.
12. Indien binnen deze termijn de benodigde gegevens nog niet beschikbaar zijn, zal Opdrachtnemer binnen deze termijn de beschikbare gegevens aan Opdrachtgever aanleveren, met een inschatting van de termijn waarop de overige gegevens beschikbaar zullen komen of de reden waarom deze gegevens niet kunnen worden aangeleverd.
13. Opdrachtnemer zal Opdrachtgever voortdurend op de hoogte houden van actuele ontwikkelingen rondom het datalek en van de maatregelen die Opdrachtnemer treft om de gevolgen van het incident te beperken en herhaling te voorkomen.
14. Opdrachtgever zal Opdrachtnemer op de hoogte houden van wijzigingen in de contactpersonen die aanspreekpunt zijn in het geval van een (mogelijk) datalek.

Communicatie

15. Alle communicatie zowel intern als extern over het datalek verloopt via de Opdrachtgever;
16. De Opdrachtgever stelt vast of de pers dan wel andere derden geïnformeerd moet worden;

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Aard van de Inbreuk in verband met Persoonsgegevens , waaronder betrokken categorie en aantal betrokkenen.

De Persoonsgegevens en Betrokkene

Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens.

Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.