Stroomschema melden datalekken



Stap 1: Registreren van een beveiligingsincident

Wanneer er een beveiligingsincident wordt opgemerkt, moet dit gemeld worden via de SelfServiceDesk, ook wel Topdesk. Indien er persoonsgegevens bij betrokken zijn, is het een datalek. Voor het melden van het incident in SelfServiceDesk is een aparte instructie gemaakt. Deze werkinstructie is te vinden op het intranet.

Iedereen kan deze melding doen. Het is de bedoeling dat de melding zo snel mogelijk wordt gedaan. Ben je niet in de gelegenheid om de melding via de SelfServiceDesk te doen, neem dan direct contact op met helpdesk van de afdeling Automatisering van GGD Amsterdam (tel. 020-5.1,2,e of mail 5.1,2,e @ggd.amsterdam.nl)

Wanneer de melding is opgeslagen in SelfServiceDesk krijgt de Privacy Officer (PO) direct een bericht per e-mail en sms en gaat de PO met jouw melding aan de slag. Voor de namen bij deze functie, kijk op deze pagina op intranet.

Stap 2: Contact met Privacy contactpersoon

Indien de melding vragen oproept, neemt op verzoek van de Privacy Officer de Privacy contactpersoon van de desbetreffende afdeling contact op met de melder om meer informatie uit te vragen. Met deze aanvullende informatie wordt de melding in de SelfServiceDesk compleet.

Stap 3: Onderzoek door Privacy Officer en Information Security Officer

De privacy contactpersoon van jouw afdeling zal samen met de Privacy Officer en eventueel de Information Security Officer het datalek verder onderzoeken. Zij controleren of ze alle benodigde informatie hebben. Afhankelijk van de melding zullen ze ook contact zoeken met functioneel en/of technisch beheerders van betreffende applicaties. Vervolgens wordt de ernst van het datalek bepaald en worden maatregelen geïnitieerd of direct geïmplementeerd om herhaling te voorkomen.

Stap 4: Contact met afdelingsmanager

De manager van de afdeling waar het datalek heeft plaatsgevonden (manager van melder of van de afdeling waar een bepaalde applicatie wordt gebruikt) moet geïnformeerd worden over het datalek en de te treffen maatregelen om herhaling te voorkomen. Dit doet de Privacy contactpersoon, eventueel samen met de Privacy Officer.

Stap 5: Gevoelige datalekken

Indien het een zeer gevoelig datalek betreft, en de mogelijkheid bestaat dat het bijvoorbeeld door lokale of landelijke pers wordt opgepakt en (groot) nieuws wordt, zullen meer mensen geïnformeerd worden. Naast de directeur van de GGD, zal dan ook wellicht de stedelijke directeur en eventueel zelfs wethouder ingelicht moeten worden. Dit gebeurt, afhankelijk van de ernst, in overleg tussen Privacy contactpersoon, Privacy Officer en afdelingsmanager.

Stap 6: Risico voor betrokkene

Vastellen van wie de persoonsgegevens zijn gelekt als gevolg van het datalek en of waarschijnlijk sprake is van een risico voor deze betrokkene(n) zoals bijvoorbeeld imagoschade, identiteitsfraude of een beperking in de uitoefening van zijn of haar rechten.

Zo ja, volg stap 7.

Zo niet, ga dan verder naar stap 9.

Stap 7: Risico óf hoog risico

Indien er in de vorige stap is bepaald dat er waarschijnlijk een risico voor de betrokkene is, dient er nog een afweging gemaakt te worden.

De Privacy Officer zal in overleg met de Privacy contactpersoon de Functionaris Gegevensbescherming (FG) van de gemeente verzoeken het datalek te melden bij de landelijke Autoriteit Persoonsgegevens (AP). Dit gebeurt enkel nádat de directie van de GGD is ingelicht. Indien intern besloten is dat het datalek gemeld moet worden bij de AP, wordt het datalek dus eerst gemeld bij de FG.

Is bepaald dat er een hoog risico is voor de betrokkene(n) van het datalek? Volg stap 8.

Indien dit niet het geval is, ga dan verder naar stap 9.

Stap 8: Informeren betrokkene(n)

Bij een hoog risico zal/zullen de betrokkene(n) geïnformeerd moeten worden over het datalek dat heeft plaatsgevonden. Deze afweging wordt gemaakt door de Privacy contactpersoon en de Privacy Officer enkel na overleg met de directie. In overleg wordt bepaald wíe contact opneemt met de betrokkene(n). Dit kan ook door de afdelingsmanager opgepakt worden.

Ook dit wordt door de FG gemeld bij de Autoriteit Persoonsgegevens.

Stap 9: Reparatie datalek

Het datalek moet gerepareerd worden. Op advies van de Information Security Officer en Privacy Officer zullen er maatregelen getroffen moeten worden door de daarvoor verantwoordelijke afdelingsmanager.

De privacy contactpersoon informeert de afdeling over de doorgevoerde maatregel(en).

Stap 10: Registratie datalek

Na afronding van het datalek, wordt het incident geregistreerd in het datalekkenregister van de GGD (binnenkort gemeente). Regelmatig wordt hierover stedelijk aan de GGD directie gerapporteerd.