odijmond
OMGEVINGSDIENST IJMOND

Procedure datalekken ODIJ.

Verantwoordelijke

Directeur Omgevingsdienst IJmond

Doel:

Deze procedure beschrijft de wijze waarop de organisatie op een gecontroleerde wijze datalekken afhandelt.

De volgende stappen worden gehanteerd:

1. Het signaleren, analyseren en registreren van incidenten waarbij er sprake is van een inbreuk in verband met persoonsgegevens.
2. Het zsm nemen van correctieve en preventieve maatregelen.
3. Het inhoudelijk beoordelen en onderzoeken van het incident op mogelijke risico's voor betrokkenen.
4. Het indien nodig melden van het datalek aan de toezichthouder en betrokkenen.
5. Het registreren van het datalek in het datalekregister.

Toelichting

Toepassingsgebied
Deze procedure wordt gehanteerd bij het melden, registreren en afhandelen van (mogelijke) datalekken veroorzaakt door ODIJ dan wel van (mogelijke) datalekken die buiten de ODIJ hebben plaatsgevonden, maar waarvoor de ODIJ als verwerkingsverantwoordelijke de eindverantwoordelijkheid draagt.

Voorbeelden van datalekken:

- persoonsgegevens zijn verstuurd of afgegeven aan verkeerde ontvangers. Denk hierbij aan het versturen van een email met daarin persoonsgegevens aan de verkeerde ontvanger. De oorzaak kan een typefout zijn of omdat er in een mailprogramma een verkeerde geadresseerde wordt geselecteerd.

- poststukken waarin persoonsgegevens staan die kwijtraken of die bij de verkeerde persoon worden bezorgd en geopend retour worden verzonden.

- Laptop of usb-stick of telefoon met persoonsgegevens is kwijtgeraakt of gestolen

- Hacking, malware of phishing. Phishing is het sturen van nepmails waarbij het aanklikken van een link kan leiden tot installatie van malware (ransomware) op het systeem waardoor gegevens versleuteld worden.

  83% van de datalekken bestond in 2018 volgens de Autoriteit Persoonsgegevens uit bovenstaande datalekken.

Gebruikte termen:

Datalek
Een inbreuk in verband met persoonsgegevens: 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.
Samengevat komt het erop neer dat persoonsgegevens komen waar zij niet behoren te zijn.

Persoonsgegeven
Alle informatie over een geidentificeerde of identificeerbare natuurlijke persoon (de betrokkene).

Verwerking van persoonsgegevens

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere manier ter beschikking stellen, samenbrengen of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

Procedure

Melden

Een datalek moet intern altijd worden gemeld bij de Functionaris Gegevensbescherming (FG). Dit is Wilma Zandvliet – van Zelst (tel. 0251-263865). Ook wanneer je twijfelt of er sprake is van een datalek; meldt het bij de FG.

Bij de melding wordt zoveel mogelijk informatie over het datalek gegeven: wat is er gebeurd, welke gegevens betreft het, wie zijn de betrokkenen, inschatting van het risico, zijn er al maatregelen genomen?

Melding aan Autoriteit Persoonsgegevens (AP) en betrokkenen.

De FG beoordeelt het incident en besluit of er sprake is van een 'meldingsplichtig datalek' dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) en betrokkene(n). In deze beoordeling wordt gekeken naar de risico's die het datalek kan veroorzaken. Denk hierbij aan verlies van controle over de persoonsgegevens, identiteitsfraude, financiele verliezen, reputatieschade. De FG of zijn vervanger kan het intake-formulier interne melding datalek Omgevingsdienst IJmond gebruiken bij het intern opnemen van een datalek en het bepalen van vervolgacties.

Geen melding hoeft te worden gedaan bij AP en betrokkene door de FG als het niet waarschijnlijk is dat de inbreuk een risico voor betrokkenen met zich meebrengt. Deze datalekken moeten wel worden geregistreerd zodat daaruit lering voor de toekomst kan worden getrokken. Registratie en evaluatie zijn verantwoordelijkheid van de FG.

De FG is verantwoordelijk dat er melding wordt gedaan bij de AP (en eventueel betrokkenen) en dat dit gebeurt binnen 72 uur. De melding aan de AP bevat de aard van de inbreuk, categorieen van betrokkenen en persoonsgegevens, naam en contactgegevens van de FG, de waarschijnlijke gevolgen van de inbreuk, de maatregelen die zijn voorgesteld of genomen.
De melding wordt gedaan via https://datalekken.autoriteitpersoonsgegevens.nl
Bijgaande link geeft voorbeelden van wel/niet melden datalek:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2019_voorbeeldlijst_wel_niet_melden_datalek_def.pdf

De melding aan betrokkenen is vormvrij en bevat een omschrijving in duidelijke en eenvoudige taal van de aard van de inbreuk, naam en contactgegevens van de FG, de waarschijnlijke gevolgen van de inbreuk en de maatregelen die zijn voorgesteld of genomen.

Herstellen

De FG zal samen met de benodigde expertise (bv de IT mensen) de oorzaak van het datalek achterhalen en deze indien mogelijk herstellen. De correctieve en preventieve technische en organische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk(en) te voorkomen worden vastgelegd in het datalekregister.

Registreren (Datalekregister)

De FG houdt het datalekregister bij waarin alle datalekken die zich voordoen binnen en buiten (verwerkers) de organisatie worden geregistreerd.