

Jaarverslag Datalekken 2016

Op 1 januari 2016 is de wet Meldplicht datalekken in werking getreden. Met de invoering van deze wet hebben wij de verplichting gekregen om datalekken te melden. In deze infographic informeren wij u over de datalekken en andere incidenten die in 2016 plaatsvonden in Helmond.



Wat is een datalek?

Bij het uitvoeren van de gemeentelijke taken worden persoonlijke gegevens van burgers verwerkt. De Wet bescherming persoonsgegevens Wbp (en de desbetreffende materiewet) geven de kaders aan waarbinnen deze persoonsgegevens mogen worden verwerkt.

Zodra er een fout optreedt in de beveiliging, waarbij mogelijk persoonsgegevens verloren zijn gegaan of onrechtmatig ingezien, is er sprake van een incident. Wanneer er daadwerkelijk persoonsgegevens verloren zijn gegaan of onbevoegd worden verwerkt, is er sprake van een datalek.

Zijn de betrokken persoonsgegevens gevoelig? Dan moet het lek gemeld worden bij de Autoriteit Persoonsgegevens (AP).

Loopt de betrokkene bovendien een grote kans dat hij nadelige gevolgen zal ondervinden? Dan moet ook deze betrokkene worden ingelicht.

Ahaa....!

Voorbeelden van gevoelige gegevens en de nadelige gevolgen die kunnen optreden:

- Stigmatisering: Informatie over je prestaties, zoals een beoordeling
- Identiteitsfraude: BSN
- Financiële schade: Informatie over het feit dat je een uitkering hebt

Voorbeelden van datalekken zijn:

- het verlies van een usb stick met daarop persoonsgegevens
- een inbraak op onze systemen door een hacker
- het binnen onze organisatie onbevoegd verwerken van persoonsgegevens (bijvoorbeeld het onbevoegd raadplegen van Suwinet)

16 incidenten zijn onderzocht (7 hiervan betroffen geen persoonsgegevens)



De 9 datalekken zijn getoetst op nadelig effect voor betrokkenen

8 gemeld bij AP

De 8 meldingen zijn beoordeeld op daadwerkelijke schade op betrokkenen

verkeerd adres



1

door derden



1



2

daadwerkelijk bij een ander aangekomen

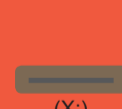
Enkele personen kregen te horen dat poststukken waren omgewisseld.



Maatregelen

Naar aanleiding van deze evaluatie zijn de volgende maatregelen getroffen:

- Aanscherping van antivirus software
- Een aantal voorzieningen zijn ontoegankelijk gemaakt



(X:)



webmail, geen toegang tot privé mail op gemeentelijke devices



Fabebook

- Acties om bewustwording te vergroten



Versturen van fakemail



geven van presentaties

- Bezig om informatieveiligheid en privacy structureel te borgen over de organisatie

