# Protocol datalekken

De AVG bepaalt dat datalekken direct, doch binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (’AP’), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens gelekt zijn, dan is de melding meestal noodzakelijk.

## Wat is een datalek?

Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Voorbeelden van persoonsgegevens die mogelijk onterecht in handen vallen van derden kunnen zijn:

* Kwijtraken van een USB -stick
* Diefstal van een laptop
* Inbraak door een hacker
* Persoonsgegevens per ongeluk gepubliceerd
* Hacking, mailware of fishing
* Persoonsgegevens aan verkeerde persoon verstuurd
* Calamiteiten zoals brand in een datacentrum

## Contactpersoon aanwijzen

Henk Salome is binnen MKB Westland de contactpersoon (hierna: ‘Contactpersoon”) aan wie eventuele datalekken gemeld moeten worden.

## Informeren Contactpersoon

Bestuursleden en personeel binnen MKB Westland dienen zich er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de Contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan (**bijlage 1**).

## Registreren datalekken

MKB Westland houdt een eigen registratie van de datalekken bij die zich binnen MKB Westland hebben voorgedaan. Op deze manier kan AP controleren of MKB Westland aan de meldplicht heeft voldaan.

Op SharePoint heeft MKB Westland een logboek waarin zij de datalekken registreren. Ook zal er per datalek een folder worden aangemaakt waarin informatie over het datalek kan worden opgeslagen (**bijlage 2**).

## Uitvoeren van het stappenplan Datalekken

De Contactpersoon draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een datalek optreedt dienen de stappen in het stappenplan Datalekken doorlopen te worden.

Vastgesteld d.d. 14 mei 2018

## Bijlage 1: Stappenplan datalekken

|  |  |  |
| --- | --- | --- |
| **Processtappen** | **Activiteit** | **Verantwoordelijke persoon** |
| 1 | Er wordt een (mogelijk) datalek ontdekt | * Maak direct intern melding van (mogelijke) datalek
* Informeer de Contactpersoon
 | Degene die het (mogelijke) datalek ontdekt |
| 2 | Beoordeel het datalek | * Onderzoek het beveiligingsincident
* Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden
* Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn
* Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden
 | Opdrachtverantwoordelijke/Contactpersoon |
| 3 | Bestrijdt het datalek | * Stop het datalek als het nog kan
* Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken
* Leg de acties van de genomen maatregelen vast in het logboek
 | Opdrachtverantwoordelijke/Contactpersoon |
| 4 | Vaststellen impact datalek | * Onderzoek het datalek en de gevolgen daarvan
* Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik
* Onderzoek de omvang van de gelekte gegevens
* Beoordeel welke impact het lek kan hebben op de betrokken personen
* Stel vast wat de nadelige gevolgen kunnen zijn
 | Opdrachtverantwoordelijke/Contactpersoon |
| 5 | Vaststellen Meld en Herstelaanpak | * Bepaal aanpak/informeren AP
* Bepaal aanpak/informeren betrokkenen
* Bepaal acties voor nazorg betrokkenen
* Bepaal acties voor belang van de organisatie
* Bepaal acties voor verbetering beveiliging
 | Opdrachtverantwoordelijke/Contactpersoon |

|  |  |  |
| --- | --- | --- |
| **Processtappen** | **Activiteit** | **Verantwoordelijke persoon** |
| 6 | Melden AP\* | * Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur
* Melding via de website van het AP
* Van tevoren kan het Meldformulier Datalekken gebruikt worden
 | Contactpersoon |
| 7 | Melden betrokkenen\*\* | * Melding via bijvoorbeeld e-mail/telefonisch
* Meedelen wat er is gebeurd, welke persoonsgegevens gelekt zijn en wat de mogelijke gevolgen van het datalek kunnen zijn.
* Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen
 | Opdrachtverantwoordelijke/Contactpersoon |
| 8 | Uitvoeren herstelwerkzaamheden | * Herstel het datalek
* Verbeteren van de beveiliging
* Lever nazorg aan de betrokkenen
 | Opdrachtverantwoordelijke/Contactpersoon |
| 9 | Optimaliseer het beveiligings- en het Datalek proces | * Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken
 | Opdrachtverantwoordelijke/Contactpersoon |

\* Melding aan de AP kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Contactpersoon betrokken moeten worden.

\*\* Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Contactpersoon betrokken moeten worden.