



# Dorpsraad “Rondon de Plassen”

Opgericht : 24 augustus 2011 Website: [www.rondondeplassen.nl](http://www.rondondeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondondeplassen.nl](mailto:secretariaat@rondondeplassen.nl)

## Protocol Datalekken

### Inhoud

1: Inleiding .....	2
2: Wat is een datalek?.....	2
3: Contactpersoon aanwijzen .....	2
4: Informeren medewerkers .....	2
5: Uitvoeren van het stappenplan Datalekken .....	3



# Dorpsraad “Rondon de Plassen”

Opgericht : 24 augustus 2011 Website: [www.rondondeplassen.nl](http://www.rondondeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondondeplassen.nl](mailto:secretariaat@rondondeplassen.nl)

## 1: Inleiding

De AVG bepaalt dat datalekken direct, 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.

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

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.

## 2: Wat is een datalek?

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 gelect zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelect 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

## 3: Contactpersoon aanwijzen

De organisatie moet een eigen contactpersoon aanwijzen aan wie eventuele datalekken gemeld moeten worden. Dit kan bijvoorbeeld een bestuurslid of de Functionaris Gegevensbescherming zijn. (hierna: ‘Contactpersoon’). Voor de dorpsvereniging Rondon de Plassen is hiervoor René Spaans aangewezen.

## 4: Informeren medewerkers

Medewerkers binnen de organisatie 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 aangewezen Contactpersoon, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.



# Dorpsraad “Rondom de Plassen”

Opgericht : 24 augustus 2011 Website: [www.rondomdeplassen.nl](http://www.rondomdeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondomdeplassen.nl](mailto:secretariaat@rondomdeplassen.nl)

## 5: Uitvoeren van het stappenplan Datalekken

De binnen de organisatie aangewezen 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.

### STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	<ul style="list-style-type: none"> <li>- Maak direct intern melding van (mogelijke) datalek</li> <li>- Informeer de verantwoordelijke Contactpersoon</li> </ul>	Medewerker die het ontdekt
2. Beoordeel het datalek	<ul style="list-style-type: none"> <li>- Onderzoek het beveiligingsincident</li> <li>- Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden</li> <li>- Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn</li> <li>- Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden</li> </ul>	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
3. Bestrijdt het datalek	<ul style="list-style-type: none"> <li>- Stop het datalek als het nog kan</li> <li>- Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken</li> <li>- Leg de acties van de genomen maatregelen vast in het dossier</li> </ul>	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
4. Vaststellen impact datalek	<ul style="list-style-type: none"> <li>- Onderzoek het datalek en de gevolgen daarvan</li> <li>- Onderzoek de aard van de gegevens die gelekt zijn. Bijv.</li> </ul>	Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de



# Dorpsraad “Rondon de Plassen”

Opgericht : 24 augustus 2011 Website: [www.rondondeplassen.nl](http://www.rondondeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondondeplassen.nl](mailto:secretariaat@rondondeplassen.nl)

	<p>gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik</p> <ul style="list-style-type: none"> <li>- Onderzoek de omvang van de gelekke gegevens</li> <li>- Beoordeel welke impact het lek kan hebben op de betrokken personen</li> <li>- Stel vast wat de nadelige gevolgen kunnen zijn</li> </ul>	<p>beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon Functionaris Gegevensbescherming</p>
5. Vaststellen Meld en Herstelaanpak	<ul style="list-style-type: none"> <li>- Bepaal aanpak/informereren AP</li> <li>- Bepaal aanpak/informereren betrokkenen</li> <li>- Bepaal acties voor nazorg betrokkenen</li> <li>- Bepaal acties voor belang van de organisatie</li> <li>- Bepaal acties voor verbetering beveiliging</li> </ul>	<p>Manager van afdeling waar binnen het datalek heeft plaatsgebonden Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon Functionaris Gegevensbescherming</p>
6. Melden AP*	<ul style="list-style-type: none"> <li>- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur</li> <li>- Melding via de website van het AP</li> <li>- Van tevoren kan het Meldformulier Datalekken gebruikt worden</li> </ul>	<p>Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur</p>
7. Melden betrokkenen**	<ul style="list-style-type: none"> <li>- Melding via bijvoorbeeld brief</li> <li>- Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn.</li> </ul>	<p>Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur Marketing/communicatie</p>



# Dorpsraad “Rondon de Plassen”

Opgericht : 24 augustus 2011 Website: [www.rondondeplassen.nl](http://www.rondondeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondondeplassen.nl](mailto:secretariaat@rondondeplassen.nl)

	<ul style="list-style-type: none"><li>- Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen</li></ul>	
8. Uitvoeren herstelwerkzaamheden	<ul style="list-style-type: none"><li>- Herstel het datalek</li><li>- Verbeteren van de beveiliging</li><li>- Lever nazorg aan de betrokkenen</li></ul>	Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT) Aangewezen contactpersoon
9. Optimaliseer het beveiligings- en het Datalek proces	<ul style="list-style-type: none"><li>- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken</li></ul>	Aangewezen contactpersoon Functionaris Gegevensbescherming Bestuur Manager van de afdeling die verantwoordelijk is voor de beveiligingsincidenten (bijvoorbeeld IT)

\* Melding aan de Autoriteit persoonsgegevens 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 geleepte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn geleept van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn geleept. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming 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 geleepte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) geleept 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 Functionaris Gegevensbescherming betrokken moeten worden.



# Dorpsraad “Rondon de Plassen”

Opricht : 24 augustus 2011 Website: [www.rondondeplassen.nl](http://www.rondondeplassen.nl)

Secretariaat : Kerkpad 33, 2461 TJ Papenveer

E-mail : [secretariaat@rondondeplassen.nl](mailto:secretariaat@rondondeplassen.nl)

## **Verwerker**

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken terstond (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.