Meldplicht datalekken, 1-uurs melding voor functionarissen/vrijwilligers bij de Hervormde Gemeente Veenendaal

1) **Waarom ontvang je instructie over de meldplicht datalekken?**

   Met ingang van 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens (hierna Wbp) in werking getreden die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven die persoonsgegevens verwerken, datalekken moeten melden aan de Autoriteit Persoonsgegevens (AP). In voorkomende gevallen ben je als medewerker/vrijwilliger ook verplicht mee te werken aan het proces van melding aan de AP en het adequaat informeren van leden resp. betrokkenen.

2) **Wat zijn persoonsgegevens?**

   Persoonsgegevens zijn alle gegevens die direct herleidbaar zijn tot een bepaald individu. Dat kan zijn een naam, adres, telefoonnummer, IBAN, etc. Bij twijfel ga je ervan uit dat informatie over mensen persoonsgegevens zijn.

3) **Wat is een datalek of beveiligingsincident?**

   Er is sprake van een beveiligingsincident, en dus een potentieel datalek, als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een beveiligingsincident zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Onder onrechtmatige vormen van verwerking van persoonsgegevens vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan.

4) **Wanneer melden van een beveiligingsincident?**

Bij een beveiligingsincident gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij Hervormde Gemeente Veenendaal, zonder dat dit de bedoeling was. Elk beveiligingsincident moet aan/naar privacy@hgv-kb.nl worden gemeld. Enkele voorbeelden van inbreuken op de beveiliging die moeten worden gemeld zijn: a) verlies of diefstal van USB/DVD/CD/LAPTOP met persoonsgegevens, b) een inbraak door een hacker, c) verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden, d) verlies van data zonder beschikbaarheid van back-up, c) een malware-besmetting.

5) **Klopt het dat een medewerker niet zelfstandig een melding mag doen bij de AP of aan de betrokkenen?**

Ja, dat klopt. De wettelijke meldplicht datalekken richt zich tot de verantwoordelijke binnen Hervormde Gemeente Veenendaal voor de verwerking van persoonsgegevens. Het is dus aan de hiertoe bevoegde om te bepalen of er sprake is van een inbreuk op de beveiliging. En of die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

De afweging of een datalek moet worden gemeld aan de toezichthouder AP en of betrokkenen hierover moeten worden geïnformeerd, is een besluit dat de directie moet nemen, op basis van de door jou verstrekte informatie en haar eigen inschatting.

6) **Zijn er consequenties aan het niet, niet tijdig of niet volledig melden van een datalek verbonden?**

Overtreding van de meldplicht datalekken, zoals vermeld in de Wbp, kan door de AP worden bestraft met een zeer hoge boete, een percentage van de jaaromzet van een organisatie.

Formulier voor 1-uurs melding van een beveiligingsincident aan Hervormde Gemeente Veenendaal

Naam functionaris/vrijwilliger:	
Mobiel telefoonnummer:	
E-mailadres:	
Geef een beschrijving van het incident, waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan:	
Wanneer vond de inbreuk plaats? (Datum & tijd)	
Wat is de aard van de inbreuk? (Meerdere antwoorden mogelijk)	○ Lezen (vertrouwelijkheid) (bijv. inzien salarissen) ○ Kopiëren (bijv. e-mailadres gebruiken voor ander doeleind) ○ Veranderen (integriteit) ○ Verwijderen of vernietigen (beschikbaarheid) ○ Diefstal ○ Nog niet bekend
Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk?	

Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	Minimaal: Maximaal:
Om welke typen persoonsgegevens gaat het? Je kunt meerdere mogelijkheden aankruisen)	○ Naam-, adres- en woonplaatsgegevens ○ Telefoonnummers ○ E-mailadressen of andere adressen voor elektronische communicatie ○ Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of registratienummer) ○ Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer) ○ Burgerservicenummer (BSN) of sofinummer ○ Paspoortkopieën of kopieën van andere legitimatiebewijzen ○ Geslacht, geboortedatum en/of leeftijd ○ Bijzondere gegevens (zoals medische gegevens etc.) ○ Overige gegevens, namelijk (vul aan):
Zijn de persoonsgegevens versleuteld of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?	
Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?	

Is deze melding naar jouw mening compleet of volgt nog aanvullende informatie over de inbreuk?	
Zijn er externe partijen (bijvoorbeeld leveranciers) bij dit beveiligingsincident betrokken? Zo ja, welke?	
Hebben / heeft deze externe partij(en) al zelfstandig een melding gedaan bij de AP? (Dit is niet wenselijk. Deze instructie dan ook niet geven.)	