# **Stappenplan: wat te doen bij een datalek?**

Stappenplan van de Hersteld Hervormde gemeente (naam gemeente) hoe te handelen bij het vermoeden van een datalek.

**Stap 1: Bij het vermoeden van een datalek: waarschuw direct de AVG-contactpersoon**

Als u *vermoed* dat er sprake is van een datalek, neem dan zo snel mogelijk contact op met de contactpersoon AVG binnen onze gemeente (naam, email, telefoonnummer).

**Stap 2: Contactpersoon beantwoordt de vraag: is er sprake van een datalek?**

De eerste vraag die de contactpersoon moet beantwoorden is, of er inderdaad sprake is van een datalek. Daarvoor gelden drie criteria:

1. Gaat het om persoonsgegevens?
2. Zijn deze persoonsgegevens blootgesteld aan misbruik of verlies?
3. Is deze blootstelling te wijten aan een inbreuk op de beveiliging?

Als alle drie de vragen met ‘ja’ worden beantwoord, is er sprake van een datalek.

**Stap 3: Contactpersoon beperkt zo goed mogelijk de schade.**

Als er inderdaad persoonsgegevens zijn gelekt, is het van belang vast te stellen om welke gegevens het precies gaat en wie er toegang gehad hebben tot de gegevens.

De contactpersoon kijkt of het mogelijk is de datalek te beëindigen en de schade te beperken. Zo ja, dan moeten deze maatregelen onmiddellijk worden genomen.

**Stap 4: Contactpersoon beoordeelt of het datalek gemeld moet worden bij de Autoriteit Persoonsgegevens.**

In principe moet elk datalek worden gemeld bij de toezichthouder in Nederland, de Autoriteit Persoonsgegevens. Een uitzondering is als het onwaarschijnlijk is dat er risico’s zijn voor de privacy van betrokkenen. Door die uitzondering hoeven onschuldige datalekken niet gemeld te worden.

De contactpersoon zal hiervan een inschatting moeten maken. Besluit hij dat het datalek meldingsplichtig is, dan moet het lek ***binnen 72 uur*** ***na ontdekking*** bij de Autoriteit Persoonsgegevens worden gemeld. De AP heeft daarvoor een [speciaal meldformulier](https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1) beschikbaar gesteld. U riskeert een boete als u een datalek niet meldt, terwijl dat wel had gemoeten.

**Stap 5: Contactpersoon beoordeelt of het datalek gemeld moet worden bij de betrokkenen.**

Betrokkenen zijn de mensen over wie de persoonsgegevens gaan. Een datalek moet aan hen worden gemeld als het lek waarschijnlijk een groot risico voor hen oplevert. De melding aan de betrokkenen bevat dezelfde informatie als die aan de toezichthouder.

**Stap 6: Contactpersoon registreert het datalek in een register.**

Elk datalek, ook die niet hoeven te worden gemeld, moet worden vastgelegd in een speciaal ‘datalekregister’. De volgende gegevens worden genoteerd:

1. Wat er precies is gebeurd.
2. Welke gevolgen dit (vermoedelijk had) voor betrokken personen.
3. Welke maatregelen zijn genomen om die gevolgen te stoppen of te beperken.
4. Welke maatregelen zijn genomen om een datalek in de toekomst te voorkomen.