**Procedure voor het melden van datalekken en het ontvreemden van persoonsgegevens na bijvoorbeeld inbraak.**

 Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig vooraf procedures met elkaar af te spreken. Wat staat hierin:

•**Wat is een datalek**;

We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Preciezer: een beveiligingsinbreuk waarbij persoonsgegevens verloren gaan of ongeoorloofd overhandigd, gezien of gewijzigd zijn. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte ledenlijst evengoed een datalek vormen.

Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.

Extra ter informatie:

Als een bedrijfstelefoon verloren of gestolen wordt, dan is dat mogelijk een datalek. Als een privé-telefoon kwijtraakt is er geen datalek (de AVG is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend persoonlijke of huishoudelijke doeleinden).

•**Bij wie in de organisatie een datalek gemeld moet worden;**

Als er sprake is van een datalek dient de gegevensverantwoordelijke (bijv. de coördinator van een werkgroep, coördinator buurtapp, een bestuurslid of de websitebeheerder) dit direct te melden bij een van de bestuursleden van de vereniging Dorpsbelangen De kiel.

**•Wie checkt wat er gelekt is;**

Indien er sprake is van een datalek of het ontvreemden van persoonsgegevens middels inbraak dient het bestuur direct bij elkaar geroepen te worden. De bijeengeroepen bestuursleden checken en inventariseren de ernst van de melding van het datalek of ontvreemding van persoonsgegevens middels inbraak.

**•Hoe in kaart gebracht wordt wat de gevolgen zijn voor de personen van wie de persoonsgegevens gelekt zijn;**

Er moet een risicoanalyse worden opgesteld. Dit houdt o.a.in:

* In welke mate is er eventuele persoons/privacyschade rondom de gelekte of vervreemde persoonsgegevens van de leden van Dorpsbelangen De Kiel.
* Wat zijn de gevolgen voor de leden waarvan de persoonlijke gegevens zijn gelekt of vervreemd.
* Hoe worden gedupeerde leden geïnformeerd en door wie.

**•Wel of niet melden aan de autoriteiten persoonsgegevens.**

Het bestuur van de vereniging Dorpsbelangen De Kiel kan na een risicoanalyse bepalen of zij een melding doen bij de autoriteiten persoonsgegevens of zij zelf een melding aanmaken in haar eigen “datalek dossier”.

Wat zijn de voorwaarden voor een melding aan de autoriteiten persoonsgegevens.

Een datalek moet gemeld worden bij de toezichthouder als er sprake is van een inbreuk op de beveiliging van persoonsgegevens. De inbreuk moet een aanmerkelijk risico opleveren tot nadelige gevolgen voor persoonsgegevens. De inbreuk leidt tot diefstal, verlies of misbruik van persoonsgegevens.

**Elk datalek -ook al is die niet meldingsplichtig - moet worden opgenomen in een eigen datalekkenregister. Naast de informatie over het lek zelf en de genomen maatregelen moeten de overwegingen voor het wel of niet melden worden opgenomen.**

**Als het datalek waarschijnlijk een hoog risico inhoudt, moet de betrokkene geïnformeerd worden (art 34 AVG).**

**Er hoeft niet gemeld te worden als het niet gaat om persoonsgegevens van gevoelige aard en/of er geen sprake is van (de kans op) ernstig nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens.**

**•Wie de melding doet bij de Autoriteit Persoonsgegevens.**

Als het bestuur van Dorpsbelangen De Kiel unaniem besluit om een melding aan de toezichthouders van de autoriteit persoonsgegevens te doen uitgaan, kan dit door de secretaris worden gedaan. Indien de secretaris afwezig is zorgt de voorzitter voor de afwikkeling van genoemde melding.