Grip op de Knip Katwijk

Algemene Verordening Persoonsgegevens (AVG)

Grip verzamelt gegevens over haar schuldhulpmaatjes, bestuursleden, organisaties en privépersonen waarmee wordt samengewerkt. Dit betreft naam, adres, woonplaats, telefoon en e-mail. Doel is de stichting op een normale wijze te kunnen laten functioneren. Daarnaast worden gegevens verzameld van hulpvragers die worden verwerkt in het Hulpvragersysteem (HVS) van de Vereniging SchuldHulpMaatje Nederland (VSN). Dit HVS voldoet aan de eisen van het AVG en valt onder de verantwoordelijkheid van de landelijke vereniging.

1. Het bestuur van Grip is verantwoordelijk voor de bescherming van verzamelde persoonsgegevens.
2. Het overzicht van persoonsgegevens is opgenomen in een verwerkingsregister.
3. Er worden geen bijzondere persoonsgegevens verzameld (zoals godsdienst, levensovertuiging, ras, gezondheid en dergelijke).
4. Maatjes, instanties en personen waarmee Grip samenwerkt worden geïnformeerd dat hun NAW-gegevens, e-mail en telefoonnummer worden verzameld voor een doelmatig werkende organisatie. Hulpvragers worden bij de intake geïnformeerd dat hun adres en financiële gegevens worden verzameld in het HVS om efficiënt schuldhulpverlening te kunnen geven. De hulpvragers ondertekenen daarbij een formulier waarbij zij hiervoor toestemming geven. Een privacy-statement staat op onze website www.gripopdeknipkatwijk.nl vermeld.
5. Maatjes en hulpvragers die de gegevens willen inzien die Grip verzamelt kunnen dit opvragen bij de coördinator. Organisaties en privépersonen waarmee worden samengewerkt kunnen dit bij de secretaris doen.
6. De persoonsgegevens van de hulpvragers worden bewaard in het HVS. Gegevens van afgeronde hulpvragen worden na twee jaar vernietigd. De coördinatoren verzamelen oudere, geanonimiseerde statistische gegevens over hulpvragers. De coördinatoren en bestuursleden bewaren op hun huiscomputer met back-up systeem NAW-gegevens van maatjes en organisaties en privépersonen waarmee wordt samengewerkt om de organisatie doelmatig te kunnen laten functioneren. Deze computers zijn beveiligd met een antivirus programma.
7. Het HVS is door VSN beveiligd.
8. Het HVS kent een rollenstructuur en wordt beheerd door de coördinatoren, zij kunnen alle verzamelde data inzien. Maatjes hebben slechts toegang tot de gegevens van de hen toegewezen hupvrager(s). De rollenstructuur houdt in dat men slechts toegang heeft tot data die men nodig heeft om zijn/haar taak te kunnen uitvoeren. Coördinatoren en bestuursleden hebben toegang tot de NAW-gegevens van maatjes, organisaties en privépersonen waarmee wordt samengewerkt.
9. De functionaris voor de gegevensbescherming binnen Grip is de secretaris.
10. Grip heeft een datalek procedure opgesteld die als bijlage bij deze uitwerking is opgenomen

Bijlage 1

Datalek procedure Grip op de Knip Katwijk

Hoe te handelen bij een datalek?

In dit document wordt aan de hand van een stappenplan beschreven hoe *Grip op de Knip* omgaat met een **datalek**.

Definitie: er is sprake van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot de gegevens zouden mogen hebben.
Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk.

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan en worden gedocumenteerd door **contactpersoon bescherming persoonsgegevens.** De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van Grip op de Knip Katwijk.

Randvoorwaarde bij deze procedure is dat alle medewerkers, vrijwilligers en leveranciers (bewerkers) op de hoogte zijn van de datalekprocedure.

Stap 1:

Actie melder:
Vaststellen of er sprake is van een datalek en zo ja, zo snel mogelijk melden bij contactpersoon bescherming persoonsgegevens. Zowel telefonisch als per mail.
Wanneer de inschatting is dat het om een datalek met ernstige gevolgen gaat, meteen melden.
Anders de eerstvolgende mogelijkheid binnen kantoortijden.

Toelichting:
Er is sprake van een datalek wanneer persoonsgegevens verloren zijn gegaan of er sprake is van onrechtmatige verwerking of een beveiligingsincident.
Voorbeelden:

- ✓ Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- ✓ Technisch falen (fouten of bugs in software, verlate updates, storingen);
- ✓ Menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);
- ✓ Verloren of gestolen hardware (externe harde schijf, USB-stick, server-apparatuur of laptop);
- ✓ Verzenden van e-mail naar meerdere gebruikers met openbaring van e-mailadressen;
- ✓ Calamiteit (brand datacentrum, wateroverlast)

Noot: Controle op hacks of malware wordt zoveel mogelijk geautomatiseerd.

Contactgegevens voor melding:

P.J. Vellekoop (contactpersoon bescherming persoonsgegevens)
Mobiel: 06-22313080
Mailadres: pietvel@outlook.com

Bij afwezigheid of geen gehoor:

A.J. van der Hout
Telefoon: 071-4024374
Mailadres: avanderhout@gmail.com

Stap 2:

Actie contactpersoon bescherming persoonsgegevens
Contactpersoon bescherming persoonsgegevens:

- meldt het incident bij het bestuur of de directie
- onderzoekt in eerste instantie de omvang van het incident
- roept indien nodig het responseteam bij elkaar
- start vastlegging van het incident in het logboek (onder beheer secretaris)

Toelichting
Vragen voor onderzoek:

- Wat is precies met de gegevens gebeurd?
- Wat is de aard van de getroffen persoonsgegevens?
  - ✓ Bijzondere persoonsgegevens: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens.
  - ✓ Persoonsgegevens van gevoelige aard: financieel of economisch (schulden), stigmatiserend (verslaving, naaktfoto's, specifieke problemen), inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens), gegevens die vallen onder beroepsgeheim.
- Wat is de omvang van het incident?
  - ✓ Aantal getroffen personen.
  - ✓ Hoeveelheid gegevens per getroffen persoon.
  - ✓ Worden de getroffen gegevens binnen een keten gedeeld?
- Wat is de impact op de betrokkenen (klanten/prospects/personeel)?
  - ✓ Is sprake van kwetsbare groepen (kinderen, zieken, verstandelijk beperkten, bedreigde personen)?
  - ✓ Is er kans op financieel nadeel?

Wanneer het gaat om een incident met gevolgen voor de betrokkene en/of imagoschade voor de organisatie wordt het reponse-team bij elkaar geroepen en het stappenplan verder gevolgd.
Hierbij gaat het om: of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'
Het reponseteam bestaat uit:

- Contactpersoon bescherming persoonsgegevens
- Een bestuurslid
- Communicatiemedewerker

Wanneer nodig kan advies ingewonnen worden bij een jurist.

Contactgegevens van de jurist via VSN

Wanneer het incident geen gevolgen heeft, wordt de datalekprocedure op dit moment afgerond en wordt het incident alleen geregistreerd en geëvalueerd (zie stap 7).

Stap 3:

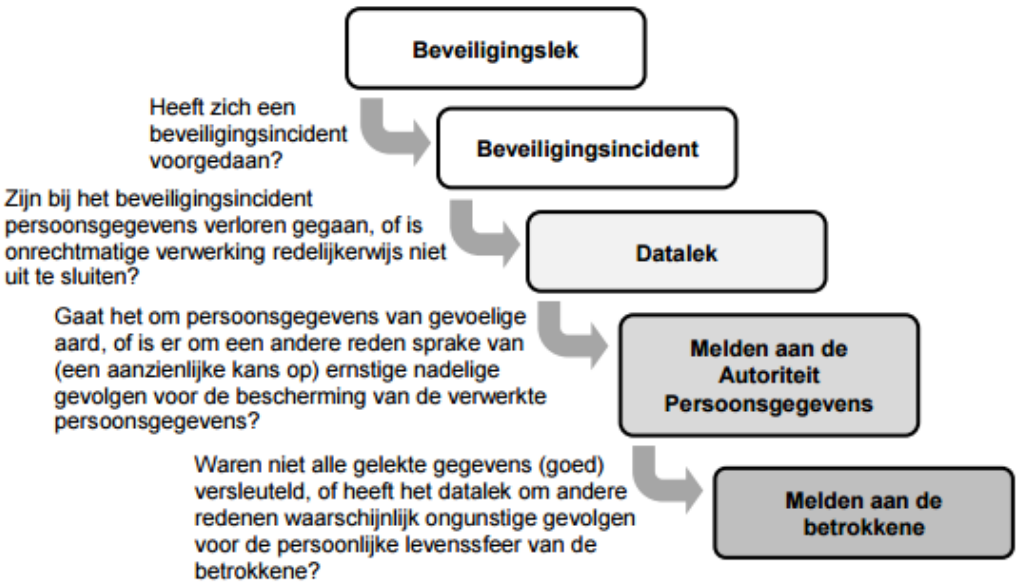
Actie responseteam
Het responseteam bespreekt het incident en neemt maatregelen met betrekking tot het datalek. Denk hierbij aan: het lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer.

Stap 4:

Actie responseteam
Het responsteam bepaalt of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en betrokkene(n).
Melden bij de Autoriteit Persoonsgegevens is verplicht indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

De personen die zijn getroffen door het datalek dienen te worden geïnformeerd indien de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer. Wanneer dit het geval is, is er altijd ook een meldplicht bij de Autoriteit Persoonsgegevens.

Toelichting
Aan de hand van de aard van de gegevens, de omvang van het incident en de impact op de betrokkenen (zie hiervoor stap 2: onderzoeken van het incident) wordt bepaald of melding noodzakelijk is. Daarbij kan onderstaand beslisschema behulpzaam zijn.



Wanneer blijkt dat het incident gemeld moet worden is dit 'onverwijld', binnen 72 uur na plaatsvinden of opmerken. De melding kan op een later moment eventueel nog aangevuld of ingetrokken worden.
Meldloket Autoriteit Persoonsgegevens:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1

Onderstaande vragen zijn behulpzaam bij het maken van een afweging of er sprake is van ongunstige gevolgen persoonlijke levenssfeer.

- Kan betrokkene last krijgen van de inbreuk, materiële of immateriële schade lijden (aard gegevens, impact, kwetsbare groep)?
- Kan betrokkene zichzelf beter beschermen als hij de inbreuk kent?

Verder:

- Bij zwaarwegende belangen kan informatie aan betrokkenen achterwege blijven.
- AP kan alsnog verlangen dat betrokkenen worden geïnformeerd
- De informatie moet betrokkenen in staat stellen om de inbreuk op hun persoonlijke levenssfeer zoveel mogelijk te beperken

Informeren hoeft niet indien de getroffen persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt (versleuteling of remote wissen).
Let op:

- Bij vernietiging (geen back-up) of aantasting (wijziging) van gegevens helpen deze beschermingsmaatregelen niet.
- Alle persoonsgegevens moeten zijn versleuteld op moment van de inbreuk.
- De versleuteling moet adequaat zijn (standaardalgoritme, sleutel niet gelekt en toekomstvast) - check publicaties ENISA (EU Agency for Network and
- Information Security) en NCSC (Nationaal Cyber Security Centrum).

Stap 5:

Actie
Het responseteam bepaalt of er maatregelen nodig zijn en zet acties uit om eventuele gevolgen/schade van het incident te beperken voor betrokkene(n).

- Wat kan SHM doen?
- Wat kan betrokkene doen?

Het responseteam bepaalt de wijze van afhandeling inclusief communicatie naar melder en betrokkene(n).

Het responseteam bepaalt of crisiscommunicatie opgestart moet worden, zowel intern als extern. Hiervoor is een crisiscommunicatieplan incl. kernboodschap opgesteld:

het crisiscommunicatieplan verloopt via VSN

Stap 6:

Actie responseteam
Het responseteam gaat na of er overige acties genomen moeten worden zoals:

- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad
- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit SHM zelf, een klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen.
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden
- Of er melding gedaan moet worden bij een eventuele verzekering en bijbehorende voorwaarden.

Stap 7:

Actie responseteam
Wanneer het incident onder controle is en er geen actie ondernomen meer hoeft te worden, wordt de procedure afgesloten.
Binnen 2 weken wordt het incident en de doorlopen procedure geëvalueerd door het responseteam. Initiatief ligt bij contactpersoon bescherming persoonsgegevens.
Doel van de evaluatie is het voorkomen van soortgelijke incidenten in de toekomst en eventuele verbeteringen van de datalekprocedure.

20 juni 2018