AVG Handleiding

Jongerenorganisatie Vrijheid en Democratie

Versie 1.1

Revisiebeheer

Versie	Revisie
1.0	Initiële publicatie van de AVG Handleiding voor besturen.
1.1	Toevoegingen: • Revisiebeheer • Bewaartermijn ledenadministratie gespecificeerd op 7 jaar.

Inleiding

Beste JOVD'er,

Sinds jaar en dag staat de JOVD voorop als het gaat om de bescherming van persoonsgegevens. Privacy is één van de speerpunten waar onze vereniging als liberale waakhond zowel in de samenleving als binnen onze organisatie naar streeft. Op dagelijkse basis werken vele leden vrijwillig mee aan het organiseren van activiteiten en het reilen en zeilen van projecten.

Onze vereniging bouwt op de energie van onze vrijwilligers, maar dit houdt tevens in dat vele handen met gegevens van onze leden werken. Hieronder vallen onder andere de afdelingsbesturen, die bijvoorbeeld nieuwsbrieven uitsturen en uitnodigingen verzenden voor afdelingsvergaderingen. Zonder het gebruik van deze gegevens kunnen veel bestuursleden hun functie niet uitoefenen.

Het beheer en gebruik van de gegevens is te allen tijde met grote zorg bewerkstelligd. Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. In de nieuwe regelgeving zijn strikte regels vastgelegd waar de JOVD als vereniging aan zal moeten voldoen.

Middels dit document, als één van de vele maatregelen die in overeenstemming met de privacy commissie zullen volgen, trachten wij u als afdelingsbestuurder in te lichten en advies te bieden met betrekking tot de nieuwe verordening. Deze handleiding verschaft u informatie over uw taken omtrent de omgang met persoonsgegevens en het handhaven van de kaders waarbinnen deze gegevens gebruikt mogen worden. Er zijn eveneens adviezen opgenomen voor het onverhoopte geval zich toch een datalek voordoet.

Als vereniging dragen wij allen de verantwoordelijkheid voor de bescherming van de persoonsgegevens van onze leden. Enkel als iedereen zich aan de omgangsregels houdt, komen wij gezamenlijk zowel onze liberale verantwoordelijkheid als juridische verantwoording na.

Hierbij hoopt het Algemeen Secretariaat der JOVD u met deze informatie goed op weg te helpen en u van de nodige informatie te voorzien voor de uitoefening van uw bestuursfunctie binnen de nieuwe wetgeving. De

Mocht u toch nog vragen hebben of heeft u twijfels, dan kunt u altijd contact opnemen met het Algemeen Secretariaat.

Het Algemeen Secretariaat wenst u veel succes!

Namens het Hoofdbestuur der JOVD,
Met vriendelijke groet,

Dorus Dijkstra
Landelijk Secretaris

Vraag en antwoord

- **Wat verandert er met de invoering van de Algemene verordening gegevensbescherming (AVG) per 25 mei 2018?**
  De belangrijkste veranderingen zijn: een versterking en uitbreiding van privacyrechten van leden, meer verantwoordelijkheden voor de JOVD en stevige bevoegdheden voor de privacytoezichthouder Autoriteit Persoonsgegevens (AP).

- **Wie is binnen de JOVD het aanspreekpunt voor privacy gerelateerde vragen?**
  De vraagbaak en het aanspreekpunt binnen de JOVD is de Landelijk Secretaris van de JOVD.

- **Wie is er verantwoordelijk voor de bescherming van persoonsgegevens van de leden?**
  Er is een gezamenlijke en gedeelde verantwoordelijkheid. De JOVD zorgt ervoor dat de voorkant up-to-date is en biedt een veilige website aan waarop ledengegevens ter beschikking worden gesteld. En waarin de ledengegevens onderhouden kunnen worden. U zorgt ervoor dat u zorgvuldig handelt binnen de afgesproken spelregels (zie later meer).

- **Wie is er aansprakelijk?**
  Mocht er iets misgaan en is er zorgvuldig gehandeld conform de spelregels, dan is de landelijke JOVD aansprakelijk. Op het moment dat iemand zich niet gehouden heeft aan de geldende spelregels of opzettelijk de regels heeft overtreden, dan kan en zal het Hoofdbestuur de betreffende persoon aansprakelijk houden voor de geleden schade.

- **Welke bestuursleden hebben er toegang tot de ledenadministratie?**
  In iedere afdeling heeft de afdelingssecretaris toegang tot de ledenadministratie van de desbetreffende afdeling.

- **Waar bewaar ik de ledengegevens?**
  De secretaris heeft toegang tot de ledenadministratie via Mijn JOVD. Mijn JOVD is een beveiligde internetomgeving. Vanuit Mijn JOVD kunt u exports maken. Deze moet u opslaan op een goed beveiligde omgeving. Dus bijvoorbeeld niet op het bureaublad van een computer waar ook anderen gebruik van maken. Vanuit Mijn JOVD kunt u een export maken. Vernietig na het gebruik ook direct de gegevens weer en laat deze niet op uw laptop staan.

- **Met wie mogen de ledengegevens worden gedeeld?**
  Ledengegevens mogen alleen gedeeld worden met door de ledenvergadering benoemde bestuursleden, wanneer een bestuurslid voor een specifiek bedoelde activiteit over die gegevens moeten beschikken. Bijvoorbeeld het algemeen bestuurslid promotie en ledenwerving die een nieuw lid welkom wilt heten via een telefoontje of per e-mail. Zij mogen de benodigde ledengegevens alleen krijgen van de secretaris.

- **Mag ik de ledengegevens ook met de afdelingsleden delen?**
  Nee, dat mag niet. De gegevens mogen alleen gedeeld worden met het daarvoor benoemde bestuurslid. U kunt natuurlijk wel aanbieden om een bericht te versturen namens een lid van de afdeling.

- **Welke gegevens mag ik als secretaris delen?**
  Beperk het delen van de gegevens tot alleen de noodzakelijke persoonsgegevens. Voor bijvoorbeeld het contact dat het bestuurslid promotie en ledenwerving wilt hebben per e-mail of telefoon. Hierbij verstrekt u alleen de gegevens die noodzakelijk zijn voor dit contact, dus bijvoorbeeld geen woonadressen.

- **Hoe deel ik de ledengegevens?**
  De persoonsgegevens worden zo beperkt mogelijk gedeeld, geëxporteerd uit het beveiligde Mijn JOVD en na afloop vernietigd door de ontvanger. Nog beter is om de gegevens niet digitaal te delen (dan zitten ze immers ook in een mailbox), maar bijvoorbeeld ter inzage te leggen bij u thuis of tijdelijk via een betaalde Google Drive.

- **Waar mogen de ledengegevens voor gebruikt worden?**
  De ledengegevens mogen alleen gebruikt worden voor de doeleinden genoemd in het privacy en cookie protocol (deze zal zo spoedig mogelijk beschikbaar worden gemaakt). Het betreft hier onder de permanente campagne/Augustus Offensief, voorzien van verenigingsinformatie, het beheren van de ledenadministratie en de financiële administratie.

- **Hoe e-mail ik veilig mijn leden?**
  Maak altijd gebruik van de BCC-functie. Pas op met het doorzenden van een reeds in BCC gestuurde email, de e-mailadressen kunnen dan alsnog zichtbaar worden.

- **Ik maak gebruik van MailChimp. Hoe zit het dan?**
  MailChimp verstuurt e-mails altijd automatisch in de BCC, dus dat is veilig. Deel als secretaris nooit het account van MailChimp met personen die geen toegang mogen hebben tot de ledengegevens.

- **Op mijn ledenvergadering gaat een lijst met namen en handtekeningen (presentielijst) rond, mag dit?**
  Dit is niet de bedoeling, want op die manier worden de ledengegevens gedeeld met alle afdelingsleden. Beter zou bijvoorbeeld zijn als een bestuurslid, de afdelingssecretaris, met een laptop de presentie bijhoudt.

- **Een persoon vraagt of u hem/haar aanmeldt als lid, mag dat?**
  Personen die lid willen worden moeten en kunnen dat zelf doen. Dit gaat gemakkelijk via onze website https://www.jovd.nl/word-jovder. Aanmelden middels een andere manier of door een derde is dus niet mogelijk.

- **Wanneer is er sprake van een datalek?**
  Hier is sprake van wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.

- **Wanneer moet ik een datalek melden?**
  U meldt altijd en zo snel mogelijk (uiterlijk binnen 24 uur) een datalek aan de Landelijk Secretaris. Ook bij twijfel vragen wij u dit altijd te doen.

- **Hoe lang bewaar ik ledengegevens in het archief?**
  Het Algemeen Secretariaat heeft de wettelijke verplichting om ledengegevens 7 jaar te bewaren. Je hoeft dus in beginsel zelf geen ledengegevens te archiveren. Er is bovendien vaak geen reden toe en de ledengegevens zijn veranderlijk. Indien archivering om bepaalde redenen wel plaatsvindt, dan moet dit onder een van de doeleinde genoemd in de privacy protocol vallen. Er is geen wettelijke bewaartermijn voor het archief, dus zorg ervoor dat u de gegevens nooit te lang bewaart.

- **Wat is het Privacy & Cookie Protocol en waar vind ik dit?**
  In de privacy protocol is nauwkeurig vastgelegd welke persoonsgegevens met welk doel gebruikt mogen worden. Iedereen die lid wordt van de JOVD of op een andere manier in onze database terechtkomt, stemt met dit privacy protocol in. Daarom is het ook niet toegestaan om een eigen ledenadministratie bij te houden: gegevens die daarin voorkomen vallen niet onder dit protocol. Het protocol wordt op zeer korte termijn beschikbaar gemaakt. Het Privacy & Cookie Protocol vindt u binnenkort op speciaal hiervoor ingerichte webpagina: https://www.jovd.nl/privacy

Omgaan met persoonsgegevens

Zorgvuldig omgaan met persoonsgegevens
De JOVD hecht er grote waarde aan dat zorgvuldig wordt omgegaan met persoonsgegevens, we hebben onszelf immers geregeld verklaard tot privacy-waakhond van Nederland, en dat de privacy van onze leden gewaarborgd is. Daar speelt u als bestuurslid een belangrijke rol in. De JOVD vraagt u daarom dringend om u te houden aan deze spelregels.

De activiteiten waarvoor persoonsgegevens nodig zijn, passen binnen de doeleinden zoals vastgelegd in de privacy protocol. Dit omvat alles wat nodig is voor het goed kunnen functioneren van een afdeling. Denk daarbij aan:

- het verzenden van verenigingsinformatie en uitnodigingen voor bijeenkomsten;
- het beheren van de ledenadministratie;
- het beheren van de financiële administratie.

Persoonsgegevens worden uitsluitend gebruikt voor de bijeenkomsten van de JOVD en worden alleen ter kennis gebracht aan degenen die voor bedoelde activiteiten over die gegevens moeten beschikken.

Bij het opstellen van deze handleiding hebben we steeds de wetgeving in acht genomen en naar aanleiding daarvan zo praktische mogelijke spelregels voor u op te stellen.

Ledenadministratie is alleen toegankelijk voor de secretaris
Voor afdelingen geldt dat enkel de secretaris van de afdeling toegang heeft tot de ledenadministratie van de afdeling via Mijn JOVD.

De secretaris wordt voor deze taken benoemd door de ledenvergadering van de afdeling. De secretaris is verantwoordelijk voor het beheer van de ledenadministratie en de bescherming van persoonsgegevens. Het is dus belangrijk dat de secretaris hiervoor waakt.

Ledengegevens alleen beperkt delen met benoemde bestuurders
Vaak hebben andere bestuursleden of leden van de afdeling persoonsgegevens nodig om hun taken uit te kunnen voeren. Hoe kan je als secretaris de bescherming van persoonsgegevens waarborgen, maar er ook voor zorgen dat de afdeling niet onnodig belemmerd wordt bij de uitoefening van bepaalde taken?

Om een afweging te kunnen maken of het delen van de ledengegevens gerechtvaardigd is, dienen onderstaande vragen bevestigend beantwoord te worden (het **vragenplan**):

1. Passen de activiteiten waarvoor persoonsgegevens nodig zijn binnen de doeleinden zoals vastgelegd in de privacy protocol?
2. Is de persoon benoemd door de ledenvergadering voor de uitvoering van deze activiteit?
3. Worden alleen die persoonsgegevens gedeeld die nodig zijn voor de uitvoering van de activiteit?

Het delen geschiedt beveiligd en na afloop vernietigen
Er worden nooit persoonsgegevens gedeeld op een wijze waardoor anderen dan de secretaris inzicht blijven houden in de ledenadministratie. De secretaris mag dus nooit de inlogcodes voor Mijn JOVD delen met een ander bestuurslid (of met welk ander lid dan ook).

Om het risico op een datalek zo klein mogelijk te houden, geven wij u de volgende tips:

- indien de secretaris digitaal inzicht verleend in de ledenadministratie door middel van bijvoorbeeld een Excel-sheet, wordt altijd vermeld dat de persoonsgegevens niet verder verspreid mogen worden en na gebruik vernietigd moeten worden;
- de gegevens die u deelt zijn gegevens die u getoetst heeft aan het "vragenplan";
- het document met de ledengegevens kunt u zelf beveiligd opslaan, bijvoorbeeld met een wachtwoord;
- nog beter is het wanneer het inzicht verlenen in de ledenadministratie gebeurt onder toeziend oog van de secretaris.

Leden alleen mailen in de BCC
Voorkom dat de ledenlijst inzichtelijk wordt voor alle ontvangers van een e-mail en stuur e-mails **altijd** in de BCC.

Geen aparte ledenadministratie bijhouden
De ledenadministratie vindt alleen plaats in Mijn JOVD. Het is niet toegestaan om een aparte ledenadministratie bij te houden. De voornaamste redenen hiervoor zijn:

- ieder lid waarvan u de gegevens via Mijn JOVD kunt raadplegen, heeft nadrukkelijk ingestemd met het gebruik van zijn gegevens conform de doeleinden uit de privacy protocol;
- Mijn JOVD is een beveiligde omgeving;
- de gegevens uit Mijn JOVD zijn altijd up-to-date.

Datalekken

Het is wettelijk verplicht om datalekken te melden. Omdat de afdelingen (zonder rechtspersoon) eenzelfde juridische entiteit vormen met de landelijke JOVD, ligt de verantwoordelijkheid datalekken te melden bij de bestuurlijk verantwoordelijke, namelijk het Hoofdbestuur van de JOVD.

De melding van een datalek aan de Autoriteit Persoonsgegevens (AP) zal vanuit één centraal punt (het Algemeen Secretariaat) plaatsvinden.

Alle datalekken moeten daarom **binnen 24 uur** gemeld worden aan het Algemeen Secretariaat bij de Landelijk Secretaris (via het speciaal daarvoor ingerichte e-mailadres: privacy@jovd.nl).

Wanneer is er sprake van een datalek?
Er moet sprake zijn van een beveiligingsincident, waarbij er daadwerkelijk persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten.

Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Met andere woorden: er is sprake van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.

Let op: dit is een ruime definitie. Er is niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een gegevensdrager in de trein, of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) telt al als datalek. Zelfs verlies van gegevens zoals bij een brand in het datacentrum waarvan geen back up beschikbaar is, ziet de wet als een datalek.

Wij vragen u daarom om alle datalekken of vermoedens daarvan te melden bij het Algemeen Secretariaat. Ook als de persoonsgegevens versleuteld zijn of wanneer u de gegevens op afstand kunt verwijderen van bijvoorbeeld een gestolen laptop, dient u melding te maken.

Wanneer meldt het Algemeen Secretariaat een datalek aan de Autoriteit Persoonsgegevens?
De wet bepaalt dat 'ernstige' datalekken zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, bij de toezichthouder gemeld moeten worden. Om binnen de genoemde 72 uur de melding te kunnen maken vragen wij u om **binnen 24 uur** de datalek aan het Algemeen Secretariaat door te geven.

Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Een paar voorbeelden uit de tweede categorie:

- inloggegevens;
- financiële gegevens;
- kopieën van identiteitsbewijzen.

Hoe handelt u richting de getroffen personen?
Naast de melding aan het Algemeen Secretariaat, dient u het lek tevens onverwijld te melden aan de personen waarvan de gegevens zijn gelekt.

Wanneer hoeft het Algemeen Secretariaat een datalek niet te melden aan de autoriteit persoonsgegevens?
Een datalek dat aan het criterium kwantitatief ernstig of kwalitatief ernstig voldoet, moet altijd gemeld worden aan de toezichthouder. Daarbij doet het er niet toe of het datalek door een fout kwam of het gevolg was van overmacht.

De beoordeling of een datalek gemeld moet worden aan de toezichthouder en/of de getroffen personen, ligt te allen tijde bij het Algemeen Secretariaat. Informeer het Algemeen Secretariaat daarom altijd, ook bij twijfel.

Welke informatie moet u over een datalek bewaren?
Wanneer u een datalek aan het Algemeen Secretariaat meldt, dient u een overzicht hiervan in uw administratie te bewaren. Dit overzicht moet de feiten en gegevens van het lek bevatten. Denk hierbij aan de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is.

Als u het datalek ook aan de getroffen personen heeft gemeld, is het belangrijk de communicatie hierover te bewaren. Voor het bewaren van de voornoemde gegevens dient u uit te gaan van een minimale bewaartermijn van één jaar.

Wat zijn de gevolgen van de AVG?
De wet kent vanaf 25 mei 2018 de mogelijkheid om boetes op te leggen wanneer een juridische entiteit niet voldoet aan de wet. Deze boetes kunnen onder meer opgelegd worden voor:

- het niet melden van een datalek terwijl dat wel moet;
- het niet op orde hebben van de beveiliging;
- het verwerken van persoonsgegevens zonder toestemming;
- export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te hebben.

Privacy protocol

In het privacy protocol is nauwkeurig vastgelegd welke persoonsgegevens met welk doel gebruikt mogen worden. Iedereen die lid wordt van de JOVD of op een andere manier in onze database terechtkomt, stemt met dit privacy protocol in.

De meest recente versie van het Privacy & Cookie Protocol vindt u binnenkort op de JOVD website.

De landelijke JOVD zal er zorg voor dragen dat alle leden geïnformeerd worden over de nieuwe verordening, tevens zal er zorg voor gedragen worden dat de website, het boekhoudsysteem, administratieve zaken en persoonsgegevens verwerkende apparatuur op het Algemeen Secretariaat aangepast worden.