Wees goed voorbereid op de nieuwe pivacywetgeving (AVG/GDPR)

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze nieuwe Europese privacywetgeving, internationaal de General Data Protection Regulation (GDPR) genoemd, geldt voor alle organisaties binnen de Europese Unie, dus ook voor Jong Nederland. De wet gaat onder andere over het bewaren en beschermen van persoonsgegevens en vervangt daarmee de Nederlandse Wet bescherming persoonsgegevens (Wbp).

WAT ZIJN DE BELANGRIJKSTE KENMERKEN VAN DE AVG?

- Bewust en transparant omgaan met de verwerking en het gebruik van persoonsgegevens.
- Persoonsgegevens enkel gebruiken voor legitieme doeleinden.
- Persoonsgegevens beschermen met geschikte beveiligingsmethoden.
- Alleen gegevens vragen die nodig zijn voor het functioneren van de organisatie.
- Personen waarvan de organisatie gegevens in haar bezit heeft, moeten in staat zijn hun gegevens in te zien of laten verwijderen.
- De opslagduur van persoonsgegevens beperken tot zo lang als nodig is voor het beoogd gebruik.
- Verplichting om datalekken te melden.

WAT ZIJN PERSOONSGEGEVENS EN WANNEER KOM IK HIERMEE IN AANMERKING?

Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats, maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst, gezondheid, strafrechtelijk verleden of seksuele geaardheid worden ook wel bijzondere persoonsgegevens genoemd.

Binnen Jong Nederland zijn er veel voorbeelden waarbij je in aanmerking komt met persoonsgegevens of privacygevoelige informatie. Bijvoorbeeld wanneer je een ledenlijst uitprint om op het clubgebouw te leggen, een overzicht maakt van alle medische gegevens voor het zomerkamp, de organisatie van de Juniorendag met de inschrijflijst informeert over de opkomst, als penningmeester de contributiefacturen verstuurt of ouders per mail een nieuwsbrief stuurt.

WAT BETEKENT DEZE WET VOOR JE JONG NEDERLAND-AFDELING?

Maak dit thema bespreekbaar om hier afspraken over te maken en deze vast te leggen in een beleidsplan dat inzichtelijk is voor je leden. Op deze manier voldoe je aan de verplichting in de wet die voorschrijft dat je moet aantonen dat je aan de wetgeving voldoet. Wanneer je als organisatie niet kan aantonen dat je voldoet aan deze wetgeving, riskeer je een boete!

HOE KAN ONZE AFDELING ZICH VOORBEREIDEN OP DE AVG?

Voor het maken van een beleidsplan kun je de volgende stappen doorlopen:

STAP 1: INVENTARISEER OVER WELKE GEGEVENS JE AFDELING BESCHIKT EN WAAR, WANNEER EN DOOR WIE DEZE GEGEVENS GEBRUIKT WORDEN.

Welke gegevens heeft je afdeling in haar bezit van (kader)leden? Op welke systemen, computers en of hardware worden de gegevens bewaard? Wie heeft er toegang tot welke gegevens? Wanneer worden deze gegevens geraadpleegd? Welke gegevens worden gedeeld en met wie?

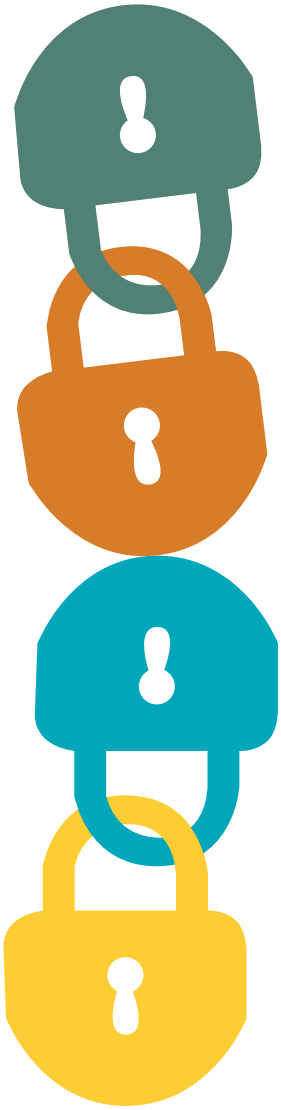
STAP 2: SCHRAP GEGEVENS DIE NIET FUNCTIONEEL ZIJN.

Op basis van de inventarisatie kun je bij elk gegeven vaststellen of het functioneel is om dit gegeven in bezit te hebben. Een afdeling die op een ledenlijst de straatnaam, het postcode en huisnummer van leden bewaart, maar alle communicatie per telefoon, sociale media en digitale nieuwsbrief laat verlopen, hoeft helemaal geen straat en huisnummer te bewaren. Het zal even wennen zijn, maar hoe minder informatie er over personen bewaard wordt, hoe moeilijker gegevens herleidbaar zijn naar een persoon en hoe minder kans op schending van privacy er is.

LET OP! Verwerken van bijzondere persoonsgegevens is verboden, tenzij hiervoor een wettelijke uitzondering is of de persoon daar uitdrukkelijk toestemming voor heeft gegeven. Dit zijn persoonsge-

gevens van gevoelige aard zoals godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of politieke partij, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, genetische en biometrische kenmerken. Onder deze laatste vallen vingerafdrukken, stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat.

Ook medische informatie, bijvoorbeeld over diabetes of allergieën, zijn bijzondere persoonsgegevens. Afdelingen hebben nu de neiging deze informatie automatisch op te slaan in een bestand. Dit is niet langer toegestaan. Deze informatie moet dus iedere keer gevraagd worden voor activiteiten waarbij dat van belang is.



STAP 3: HOE BESCHERM JE DE PERSOONSGEGEVENS: LEG WERKWIJZEN EN AFSPRAKEN VAST.

Beschrijf wat je hoe vastlegt en hoe en wie er met de gegevens omgaat en leg afspraken vast. Bijvoorbeeld: de NAW-gegevens en geboortedatums worden tweemaal per jaar door de penningmeester gebruikt om de facturen voor de contributie te maken. De facturen worden door de groepsleiders uitgedeeld aan de jeugdleden.
Als je persoonsgegevens deelt binnen of buiten je organisatie, ga dan na wat je mag delen en of hiervoor een verwerkersovereenkomst nodig is.

LET OP! Ondanks grote zorgvuldigheid, kan iedere organisatie in aanmerking komen met datalekken. Het is verplicht om datalekken binnen 72 uur na ontdekking te melden bij de Autoriteit Persoonsgegevens. Om dit zorgvuldig te doen is het handig vooraf af te spreken hoe en door wie dit gedaan wordt. Leg deze werkwijze dus ook vast. Meldingen kunnen digitaal gedaan worden bij het meldloket (datalekken.autoriteitpersoonsgegevens.nl).

Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

STAP 4: CONTROLEER SYSTEMEN, COMPUTERS EN/OF HARDWARE WAAROP GEGEVENS WORDEN BEWAARD.

Zijn de gegevens veilig opgeslagen? Wordt de software voor antivirus, antimalware en fireware tijdig bijgewerkt? Is data versleuteld? Kortom: zijn de ict-voorzieningen op orde en bestand tegen cybercriminaliteit?
Denk ook aan tablets en telefoons, log je in op een openbaar wifi-netwerk?

STAP 5: MAAK PRIVACY BESPREEKBAAR MET DE KADERLEDEN.

Zet het onderwerp op de agenda van een vergadering of organiseer een themabijeenkomst voor kaderleden. Bewustwording is namelijk erg belangrijk en het gesprek kan leiden tot extra inzichten om het privacybeleid van je afdeling bij te sturen.

Belangrijk is om het onderwerp levendig te houden. Dit kan door bijvoorbeeld jaarlijks dit onderwerp op de agenda te zetten. Je afdeling kan ook ervoor kiezen om een functionaris gegevensbescherming (FG) aan te stellen. De FG is op de hoogte van het beleid en is het aanspreekpunt voor (kader)leden, ouders/verzorgers en externen. De FG heeft als taak het onderwerp bespreekbaar te houden binnen de afdeling.

STAP 6: INFORMEER LEDEN (EN OUDERS/VERZORGERS) OVER HET PRIVACYBELEID.

Transparantie bieden en (kader)leden het recht geven hun gegevens in te zien of laten verwijderen zijn belangrijke kenmerken van de AVG. Daarom dien je leden (en ouders/verzorgers) te informeren over het privacybeleid dat je afdeling voert. Je kunt de afspraken die je hebt vastgelegd publiceren op je website, versturen via een digitale nieuwsbrief, opnemen in een inschrijfboekje en/of aan bod laten komen tijdens een ouderavond.

STAP 7: PAS GEMAAKTE AFSPRAKEN TOE.

Je afdeling heeft beleid gemaakt, dit beleid is besproken met kaderleden en leden en ouders/verzorgers zijn geïnformeerd over het beleid. Uiteindelijk moeten gemaakte afspraken uitgevoerd worden.

TOT SLOT

Ga naar onze website voor meer informatie over de AVG en om te lezen hoe de landelijke organisatie Jong Nederland omgaat met de AVG.