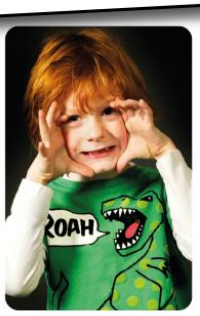
JongNL afdelingen AVG-proof!!

hoe om te gaan met persoonsgegevens binnen JongNL

VOOR MIJ JONGNL



VERSIE 1 (9 MAART 2018)

Hoe om te gaan met persoonsgegevens binnen JongNL
Hoe maak je jouw afdeling AVG-proof?

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing voor alle organisaties die gegevens van personen (persoonsgegevens) in applicaties (computerprogramma's) en computers bewaren. JongNL Limburg is zo'n organisatie en onze afdelingen ook. Wij moeten ons aan de regels in deze nieuwe verordening houden. Dat geldt zowel voor JongNL Limburg alsook voor de districten en plaatselijke afdelingen. De nieuwe verordening legt regels op over het bewaren van gegevens in digitale bestanden maar ook van gegevens in mappen op een plank of waar dan ook. Ook mappen moeten voortaan veilig worden opgeborgen zonder dat 'vreemden' daar bij kunnen.

In dit document geeft JongNL Limburg tips over de stappen die je als afdeling of district kunt nemen om te voldoen aan de eisen in de verordening.

Bij gebruik van het JongNL leden- en leidingregistratiesysteem PION sluit je als afdeling volledig aan bij de in de nieuwe verordering gestelde eisen. PION voldoet aan de gestelde eisen in de nieuwe wet.

Dit is een groeidocument. We vullen het document steeds aan. Kijk, voor je verder leest, even op www.jongnl.nl en check of er een nieuwe versie van dit document voorhanden is. Bovenaan dit document lees je welke versie je voor je hebt.

Voor vragen weet je ons te vinden via info@jongnl.nl of 0475 52 00 20.
We houden ons aanbevolen voor zinvolle opmerkingen over de inhoud van dit document.

Paul Jacobs, Leon Hoenen en Inge Craenmehr
Bestuur en bureauteam JongNL Limburg.

Dwingende adviezen voor besturen en gebruikers van persoonsgegevens in de afdelingen

- Vraag je af of de registratie van gegevens binnen je afdeling direct of indirect schade kan berokkenen aan een lid (awareness) en start daarover een gezonde discussie in het bestuur en samen met alle leiding;
- Als je gegevens download uit PION, gebruik deze dan tijdelijk en laat ze niet rondslingeren op devices (USB, flash drives, harde schijf PC), maar zorg voor verwijdering van excel-sheets, e-mails en andere applicatiesoftware waar ledeninformatie in verwerkt is;
- Gebruik geen gratis opslagmedia zoals onedrive, google drive, dropbox en zo meer. Deze zijn onvoldoende veilig of voorwaarden voor gebruik zijn in strijd met privacy regels. Een professionele Office365 Home variant heb je al voor 99euro per jaar en. Biedt vele voordelen om gegevens veilig met elkaar te delen;
- Indien iemand jouw JongNL-afdeling verlaat die toegang heeft tot PION, zorg je voor wachtwoordwijziging via JongNL Limburg (Inge Craenmehr);
- Bij twijfel of je 'goed bezig' bent met betrekking privacy, meld je je via info@jongnl.nl zodat we daar eventueel derden voor kunnen raadplegen in verband met de complexiteit;
- Ga binnen je afdeling na door een scan of checklist uit te voren waar je overal ledengegevens bewaart en of dit wenselijk/noodzakelijk is. Dit document geeft je voldoende handvatten om gestructureerd aan de slag te gaan;
- Mocht zich onverhoopt toch een situatie voordoen dat gegevens ongeoorloofd bij derden of door derden gemuteerd of geraadpleegd zijn, meld dat dan bij het bureau. We zullen dan toetsen of dit potentiële datalek gemeld moet worden bij de Autoriteit persoonsgegevens en zullen corrigerende maatregelen nemen waar mogelijk.

Hoe ga je als afdeling te werk om te voldoen aan de AVG

Stap 1 > inventariseren en weten over welke gegevens je als afdeling beschikt

Ga na welke persoonsgegevens binnen je afdeling worden verzameld en waar die worden bewaard. In de nieuwe AVG ben je verplicht te inventariseren wat jullie vastleggen, wat jullie registreren en welke persoonsgegevens jullie hoe vastleggen. Ook moeten jullie bedenken of dat wat opgeslagen wordt wel functioneel is. Je moet je dus steeds afvragen: waarom leggen we als JongNL-afdeling welke gegevens vast? Dit houdt in dat je als afdeling alleen persoonsgegevens vastlegt die je nodig hebt en dat je die gegevens alleen gebruikt waarvoor je ze verzamelt hebt.

Gevoelige gegevens die niet zondermeer vastgelegd mogen worden zijn:

- BSN-nummer
- Ras
- Geloofsovertuiging
- Medische gegevens
- Seksuele voorkeur

Het gaat hier ook om vingerafdrukken, stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat. Ook medische informatie, bijvoorbeeld over diabetes of allergieën, mag je alleen opslaan als er een wettelijke uitzondering is. Misschien heb je de neiging deze informatie automatisch op te slaan in een bestand of PION. Dat is niet langer toegestaan. Deze informatie moet dus iedere keer gevraagd

worden voor een activiteit waarbij dat van belang is. Concreet wil dat zeggen dat je na elk kamp gegevens moet verwijderen en bij elk kamp opnieuw opgevraagd worden aan de persoon of via ouders/verzorgers.

Verwerken van bijzondere persoonsgegevens is verboden, tenzij hiervoor een wettelijke uitzondering is of de persoon daar uitdrukkelijk toestemming voor heeft gegeven.

Dit zijn gegevens die niet zonder meer door een club als JongNL verwerkt mogen worden. In alle gevallen moet er een wettelijke grondslag bestaan voor de verwerking. Ter info: geen van deze gegevens worden geregistreerd in PION.

Het verwerken van herleidbare en 'gewone' persoonsgegevens moet gebeuren op basis van de gronden uit art. 8 van de wet bescherming persoonsgegevens (Wbp).

Artikel 8
Persoonsgegevens mogen slechts worden verwerkt indien:
a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Stap 2 > passende technische en organisatorische maatregelen treffen en vastleggen hoe de met data omgaat

Wat zegt de wet?
De wet eist 'passende beveiliging' van persoonsgegevens, maar dicteert niet waaraan die beveiliging exact moet voldoen.

Zet op papier wat je aan persoonsgegevens bewaart. Let op, onveranderd maar wel van belang is dat betrokkenen (leden, leiding, ouders) toestemming moeten geven voor het gebruik van hun persoonsgegevens. Alleen als daar een dringende reden van algemeen belang of wetgeving voor is, kunnen persoonsgegevens zonder toestemming worden opgeslagen. Dat is bij JongNL niet het geval. Nieuw, in de wet, is dat de betrokkenen moet weten dat zijn persoonsgegevens worden verwerkt en met welk doel. Iedereen heeft het recht zijn gegevens in te zien en aan te (laten) passen en om vergeten te worden als een lid JongNL verlaat. *Je moet dus ook uitdrukkelijk toestemming vragen om oud-leden gegevens te mogen registreren*.

Bij JongNL is helder dat persoonsgegevens noodzakelijk zijn voor het lidmaatschap en om deel te nemen aan activiteiten. Vraag leiding, bestuursleden, vrijwilligers, leden en of ouders/verzorgers of lid-gegevens opgeslagen mogen worden. Laat om deze vraag met 'ja' te beantwoorden een formulier tekenen.
Jullie hebben als afdeling een verantwoordingsplicht in de nieuwe AVG. Dat betekent dat je moet vastleggen wie, binnen de afdeling, verantwoordelijk is voor de data, aan wie informatie wordt verstrekt en

ook op welke computer (productnummer van de betreffende computer) deze wordt opgeslagen en op welke wijze deze wordt beschermd tegen virussen en hacken (informatie over relevante computerprogramma's). Jullie dienen ervoor te zorgen dat de data maar op één computer of één systeem staan. Verspreiding van data over verschillende computers of systemen, zonder dat jullie dat op papier vastleggen, kan uitgelegd worden als datalekken. Jullie moeten dus procedures opstellen om leiding toegang te geven tot informatie. Met externe gebruikers van de bestanden, zoals bijvoorbeeld de koepelorganisatie, moeten overeenkomsten worden opgesteld voor het gebruik van gegevens. JongNL Limburg heeft dat voor haar afdelingen gedaan, maar zorg hier ook voor binnen je eigen afdeling mocht dat van toepassing zijn.

Artikel 13
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Indien je het uitbesteed
Indien iemand binnen je afdeling persoonsgegevens laat verwerken door een bewerker, draagt deze bewerker zorg dat de bewerking voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. Als afdeling zie je toe op de naleving van die maatregelen. Bijvoorbeeld door een right to audit clausule. We achten de kans uitermate klein dat afdelingen persoonsgegevens door een derde laten verwerken, maar het is goed om dat even te toetsen. JongNL heeft een verwerkingsovereenkomst afgesloten met de leverancier van PION omdat zij in incidentele gevallen onderhoud doen op de applicatie en de ledengegevens.

Overige aandachtspunten
1. Beveiligingsbewustzijn
2. Fysieke en logische toegangsbeveiliging
3. Security monitoring
4. Databescherming
5. Incidentenbeheer
6. Controle op naleving

Stap 3 > meldplicht datalekken: plan voor als het fout gaat.

Wat is een datalek?
"Een aanzienlijke kans op ernstige nadelige gevolgen" voor de bescherming van de persoonsgegevens.

Voorbeelden van een datalek

JongNL zal via haar website een datalek protocol publi n het geval van een (potentieel) datalek. Dit protocol dient strikt nageleefd te worden door de afdelingen. Het 'onder de pet' houden is geen optie en kan verstrekkende nadelige gevolgen hebben.

Stap 4 > Wat nou als het wel fout gaat?

Een datalek dient binnen 72 uur gemeld te zijn bij de autoriteit 'persoonsgegevens'. Als een overtreding niet opzettelijk of door ernstig verwijtbare nalatigheid is begaan, legt Autoriteit eerst een 'bindende aanwijzing' op voordat een boete kan worden opgelegd.

Boete

- Het niet-naleven van een bindende aanwijzing kan direct worden bestraft met een boete die kan oplopen tot wel 820.000 euro of, indien dat geen passende bestraffing is, zelfs tien procent van de jaaromzet. Wordt de Wbp echter opzettelijk overtreden, dan kan dit direct tot een boete leiden.
- Met de komst van de Europese privacy verordening kan de boete oplopen tot 20 miljoen euro of 4% van de wereldwijde omzet.

Stap 5 > informeren van de leiding.

Het is niet de bedoeling dat wanneer je als bestuur de gegevensbescherming zorgvuldig beschreven hebt, de eerste de beste leider of leidster met persoonsgegevens die nodig zijn binnen JongNL, te koop gaat lopen. Ook dat zijn datalekken. Dit kan gaan om gegevens uit de bestanden van PION (ons eigen leden- en leidingregistratiesysteem), maar ook om informatie die een leider of leidster van een deelnemer of ouder/verzorger heeft gekregen. Ga dus goed na binnen je afdeling waar persoonsgegevens zich bevinden, bewerkt worden en hoe ze eventueel gedistribueerd worden.

Wat heeft JongNL Limburg, in het kader van de nieuwe wetgeving AVG, tot op heden gedaan?

1. De applicatie PION (leden- en leidingregistratiesysteem van JongNL Limburg) is ontwikkeld in Oracle en draait in een Nederlands datacentrum in Amsterdam. Oracle heeft het hoogste niveau van beveiliging voor een commercieel datacenter. Oracle zelf heeft de hoogste normen voor beveiliging van gegevens voor klanten.
2. De data verlaat Europa niet, ook niet voor backup en uitwijkdoeleinden.
3. Oracle als organisatie is ISO en NEN gecertificeerd met betrekking tot beveiliging, maar heeft ook nog aanvullende certificeringen voor de Verenigde staten. Voor meer info zie hun website www.oracle.com.
4. Het bedrijf ilionx heeft PION ontwikkeld, zij zijn ISO9001 en ISO27001 gecertificeerd en hebben een bewerkersovereenkomst opgesteld tussen ilionx en JongNL Limburg.
5. Ilionx heeft een bewerkersovereenkomst met Oracle, conform de standaard van Oracle.
6. De hosted omgeving waar PION in draait wordt wereldwijd 7x24uur gemonitord op security incidenten en maatregelen worden terstond genomen op aanvallen van buitenaf af te wenden (denk aan DDOS), eventuele security patches worden automatisch geimplementeerd.
7. De data wordt in de database encrypted opgeslagen, zodat je deze niet zonder expliciete toegang kan raadplegen.
8. De attributen (velden op de schermen) zijn gescand op privacy wetgeving; derhalve hebben we het BSN nummer verwijderd uit PION. Overige velden zijn niet privacy gevoelig. Wel adviseert JongNL Limburg de gebruikers van PION verstandig omgaan met opmerkingen en notities per lid. Privacygevoelige informatie op te slaan kan niet. Zie stap 1 in dit document.
9. In PION loggen gebruikers aan met user id en wachtwoord. JongNL Limburg werkt aan een stringenter wachtwoordwijzigingen-beleid.
10. JongNL Limburg stelt momenteel een informatiebeveiligingsbeleid op voor haar hele organisatie, eind 2018 wordt deze geïmplementeerd en zullen aanvullende maatregelen, waar nodig, getroffen worden. JongNL Limburg gebruikt Office365 voor dagelijks kantoorgebruik waarbij data binnen Europa wordt opgeslagen in de Microsoft public cloud en Yuki voor haar financiële administratie, een SAAS platform voor ondernemers waarbij data ook binnen Europa blijft.