Isala en de Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) van kracht in alle EU-lidstaten. De Nederlandse implementatie daarvan is de Algemene Verordening Gegevensbescherming (AVG). Alle organisaties die persoonsgegevens verwerken, dus ook sportverenigingen zoals Isala, krijgen dan meer verplichtingen ten aanzien van de bescherming van persoonsgegevens. De nadruk ligt daarbij – meer dan nu – op de verantwoordelijkheid van organisaties om aan te kunnen tonen dat zij zich aan de wet houden.

De AVG heeft op hoofdlijnen betrekking op vier belangrijke onderdelen:

1. De grondslag
2. Zorgvuldigheid
3. Verplichtingen
4. Rechten van betrokkenen

In de onderstaande paragrafen is per onderdeel aangegeven welke impact de invoering van de AVG heeft voor Isala en op welke wijze Isala aan de AVG-verplichtingen voldoet.

1. De grondslag

Een organisatie mag persoonsgegevens verzamelen, beheren en gebruiken (in de terminologie van de AVG heet dit 'verwerken') als dit is gebaseerd op minimaal één van de volgende grondslagen:

- Toestemming van de gebruiker
  Een rechtsgeldige toestemming voldoet aan de volgende eisen:
  - Vrijelijk gegeven – niet onder druk of nadeel bij geen toestemming
  - Ondubbelzinnig – er moet sprake zijn van een duidelijke actieve handeling
  - Geïnformeerd – duidelijk doel en aard van de verwerking, heldere rechten van betrokkenen
  - Specifiek – toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel
- Vitale belangen
  Hiervan is sprake als het verwerken van gegevens essentieel is voor iemands leven of gezondheid en de persoon zelf geen toestemming kan worden gevraagd. Denk aan medische gegevens.
- Wettelijke verplichting
  Verwerking van gegevens is noodzakelijk om aan een wettelijke plicht te kunnen voldoen.
- Overeenkomst
  Verwerking van gegevens is noodzakelijk om te kunnen voldoen aan een overeenkomst met betrokken persoon.
- Algemeen belang
  Hiervan is sprake als gegevens worden verwerkt om te kunnen voldoen aan wettelijk vastgelegde publieke taken voor het algemeen belang of openbaar gezag.
- Gerechtvaardigd belang
  De verwerking van gegevens is aantoonbaar noodzakelijk om bijvoorbeeld bedrijfsactiviteiten uit te kunnen voeren. Denk aan een personeelsadministratie.

Conclusie t.a.v. grondslag:
Isala is op basis van de grondslag **'Overeenkomst'** gerechtigd om persoonsgegevens te verwerken. Daarbij verwerkt Isala uitsluitend de persoonsgegevens die noodzakelijk zijn voor de vastlegging van de overeenkomst tussen een lid of andere geregistreerde relatie en Isala.

Indien een lid of andere relatie hier niet mee instemt kan de overeenkomst niet tot stand worden gebracht.
Voor verwerking van andere persoonsgegevens buiten de minimaal voor de overeenkomst benodigde gegevens zal Isala altijd expliciet toestemming vragen aan betrokkenen. Pas na verkregen toestemming worden deze gegeven op basis van de grondslag **'Toestemming van de gebruiker'** geregistreerd. Denk bijv. aan een (pas)foto voor op de ledenlijst. Indien geen toestemming wordt gegeven zal Isala geen (pas)foto registreren, zonder dat dit negatieve gevolgen heeft voor het betreffende lid.

Isala verwerkt geen bijzondere persoonsgegevens zoals gegevens m.b.t. etnische afkomst, politieke of religieuze overtuiging, medische gegevens, etc.

2. Zorgvuldigheid

Een organisatie is verantwoordelijk voor een zorgvuldige omgang met de gegevens van en in de eigen organisatie. Daarbij spelen de volgende factoren een rol:

- Mogelijk moet er een Functionaris Gegevensbescherming (FG) worden aangesteld.
  Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Dit is op grond van de AVG in drie situaties verplicht:
  - Voor overheden en publieke organisaties.
  - Voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Denk aan profilering van mensen, maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via 'wearables'.
  - Voor organisaties die op grote schaal bijzondere persoonsgegevens verzamelen. Denk aan iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijk verleden.

  Conclusie t.a.v. aanstelling Functionaris Gegevensbescherming:
  Isala is op basis van de van toepassing zijnde factoren niet verplicht een FG aan te stellen.

- Privacy by design en Privacy by default.
  Dit houdt in dat er bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd (Privacy by design) en dat leden bewuste keuzes maken t.a.v. de verwerking. Er mogen geen vooraf ingevulde waardes worden gebruikt (Privacy by default). Isala maakt voor de verwerking van persoonsgegevens gebruik van het geautomatiseerde verenigingspakket e-Captain. Er worden niet meer gegevens verwerkt dan minimaal noodzakelijk is om de verenigingsdoelen te realiseren. Binnen e-Captain zijn alle persoonsgegevens goed beschermd en beveiligd opgeslagen. De vastlegging, inzage, wijziging en verwijdering van deze gegevens gebeurt altijd op basis van unieke authenticatie van de gebruiker of bewerker. Uitsluitend geautoriseerde functionarissen hebben toegang tot de verwerkte persoonsgegevens en de doelen voor het gebruik zijn helder gespecificeerd. Dit is binnen e-Captain geregeld door middel van specifieke beheerprofielen met bijbehorende autorisaties.
  Formulieren die tot doel hebben om persoonsgegevens te registeren bevatten nooit vooraf ingevulde (default) waardes voor invul- of keuzevelden.

  Conclusie t.a.v. Privacy by design en Privacy by default:
  Isala voldoet aan de in de AVG gestelde criteria.

- Mogelijk is het uitvoeren van een Data Protection Impact Assessment (DPIA) verplicht.
  De DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in

kaart te brengen. Een DPIA is verplicht als aan één of meer van de volgende criteria van toepassing is:

- Beoordeling van mensen op basis van persoonskenmerken (bijv. profiling, prognoses, betrouwbaarheid, gezondheid, voorkeuren)
- Geautomatiseerde beslissingen (met wezenlijke (rechts)gevolgen voor betrokkenen)
- Stelselmatige en grootschalige monitoring (bijv. cameratoezicht openbare ruimte)
- Gevoelige gegevens (bijv. politieke voorkeuren, strafrechtelijke gegevens)
- Grootschalige gegevensverwerking (bijv. ziekenhuizen, vervoersmaatschappijen, marktonderzoeken, providers, zoekmachines)
- Gekoppelde databases (met meerdere doelen en verantwoordelijken en op een manier die betrokkenen niet redelijkerwijs kunnen verwachten)
- Gegevens over kwetsbare personen (waarbij sprak is van ongelijke machtsverhoudingen, bijv. werknemers, kinderen, patiënten)
- Gebruik van nieuwe technologieën (met grote privacy risico's, bijv. 'Internet-of-things' toepassingen)
- Blokkering van een recht, dienst of contract (bijv. een bank die persoonsgegevens verwerkt om te bepalen of iemand wel of niet een lening krijgt)

Conclusie t.a.v. verplichting tot uitvoering DPIA:
Voor de gegevensverwerking binnen Isala is geen van de in de AVG gestelde criteria van toepassing. Isala is daarom niet verplicht om een DPIA uit te voeren voor de verwerking van persoonsgegevens in de ledenadministratie.

3. Verplichtingen

Een organisatie moet technische en organisatorische maatregelen nemen om de persoonsgegevens van leden en relaties te beschermen. Deze verplichting omvat tenminste de volgende drie onderdelen:

- Bijhouden van een register met alle verwerkingen.
  Dit register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die worden verwerkt binnen de organisatie. De AVG schrijft daarbij minimaal de volgende verplichte informatie voor:
  - Naam en contactgegevens van de organisatie. In de terminologie van de AVG is dit de 'verantwoordelijke'
  - De doelen waarvoor de persoonsgegevens worden verwerkt
  - Een beschrijving van de categorieën personen van wie de persoonsgegevens worden verwerkt
  - Een beschrijving van de categorieën persoonsgegevens die worden verwerkt
  - De datum waarop de persoonsgegevens worden gewist
  - De categorieën ontvangers aan wie persoonsgegevens worden verstrekt
  - Een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens die worden verwerkt te beveiligen

Hoe voldoet Isala aan de verplichting tot het bijhouden van een register met verwerkingen:
De verplichte informatie is weergegeven in het document 'Isala Privacybeleid'. De meest actuele versie van dit document is voor alle betrokkenen beschikbaar op de Isala website.

- Opstellen van een gegevensbeschermingsbeleid
  Dit gegevensbeschermingsbeleid (ook wel Privacybeleid genoemd) is niet altijd verplicht, maar wordt sterk aanbevolen om aan zowel de betrokkenen binnen de eigen organisatie

als aan de Autoriteit Persoonsgegevens te laten zien dat wordt voldaan aan de AVG-verplichtingen. Om het nakomen van de AVG-verplichtingen aan te tonen moet het Privacybeleid tenminste de volgende informatie bevatten:

- De doelen waarvoor de persoonsgegevens worden verwerkt
- Verplichting om niet meer gegevens te verwerken dan noodzakelijk is Een beschrijving van de categorieën persoonsgegevens die worden verwerkt
- De datum waarop de persoonsgegevens worden gewist
- Welke rechten betrokkenen hebben en hoe zij deze rechten kunnen uitoefenen
- Een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens die worden verwerkt te beveiligen

Hoe voldoet Isala aan de verplichting tot het opstellen van een gegevensbeschermingsbeleid:
Het gegevensbeschermingsbeleid is weergegeven in het document 'Isala Privacybeleid'. De meest actuele versie van dit document is voor alle betrokkenen beschikbaar op de Isala website.

- De gegevens moeten beveiligd zijn
  Deze beveiliging omvat zowel organisatorische als digitale maatregelen.
  - Organisatorisch: Dit omvat alle beveiligingsmaatregelen die betrekking hebben op het verlenen van geautoriseerde toegang tot gegevens voor beheer en onderhoud door specifieke functionarissen binnen Isala. En maatregelen om te voorkomen dat gegevens in handen komen van onbevoegde derden (datalek).
  - Digitaal: Dit betreft de digitale beveiliging van gegevens binnen het verenigingspakket e-Captain. Deze beveiliging valt onder de verantwoordelijkheid van Dispi BV te Den Bosch die e-Captain levert en host. In de terminologie van de AVG is Dispi BV daarmee een zogenaamde 'bewerker'.
    Dispi BV geeft invulling aan deze digitale beveiliging door onder meer:
    - Beveiligde hosting omgeving in high tech datacenter. Servers worden altijd voorzien van noodzakelijke beveiligingssoftware en alle belangrijke updates. Hiermee wordt het risico op onbevoegde toegang tot gegevens, alsmede het ontstaan van datalekken geminimaliseerd.
    - Dagelijkse backups van alle servers. Deze worden zowel intern als extern bewaard
    - 3-traps inlogprocedure d.m.v. loginnaam, wachtwoord en pincode. Deze gegevens kunnen niet in de browser worden opgeslagen en moeten dus expliciet worden ingevoerd
    - Sessie time-out. Automatische uitlog na bepaalde periode van niet actief zijn
    - Continuïteit. De broncode van e-Captain is gedeponeerd bij een notaris in Den Bosch waar tevens een overeenkomst is gemaakt t.b.v. de continuïteit van e-Captain

  Hoe voldoet Isala aan de verplichting tot beveiliging van de gegevens:
  - De organisatorische beveiligingsmaatregelen binnen Isala zijn weergegeven in het document 'Isala Privacybeleid'. De meest actuele versie van dit document is voor alle betrokkenen beschikbaar op de Isala website.
  - De digitale en technische beveiligingsmaatregelen worden uitgevoerd door bewerker Dispi BV te Den Bosch. Isala heeft ten behoeve van deze uitvoering een Bewerkersovereenkomst afgesloten met Dispi BV. Deze Bewerkersovereenkomst voldoet aan de verplichtingen die de AVG hiertoe stelt. De meest actuele versie van dit document is voor alle betrokkenen beschikbaar op de Isala website.

4. Rechten van betrokkenen

Leden en overige relaties moeten controle kunnen uitoefenen op de gegevens die worden verwerkt. Dit houdt het volgende in:

- Recht om de gegevens in te zien
- Recht om de gegevens te wijzigen
- Recht om vergeten te worden
- Recht om gegevens over te dragen
- Recht op informatie

Hoe voldoet Isala aan de rechten van betrokkenen:

Het recht op inzage en wijziging van eigen gegevens is geborgd doordat Isala hiertoe gebruik maakt van de website functionaliteit binnen e-Captain. Ieder lid heeft de mogelijkheid om op het besloten, uitsluitend voor leden toegankelijke deel van de website de eigen gegeven in te zien en (deels) zelf te wijzigen.

Alle andere rechten zijn door middel van procedures geborgd. Deze rechten en procedures zijn opgenomen in het document 'Isala Privacybeleid'. De meest actuele versie van dit document is voor alle betrokkenen beschikbaar op de Isala website.

5. Publicatie en wijziging van dit document

De meest actuele versie van dit document is onder de naam 'Isala en de AVG' voor alle betrokkenen beschikbaar op de Isala website.

Het Isala Bestuur is verantwoordelijk voor het onderhoud op dit document. Eventuele wijzigingen op basis van wettelijke verplichtingen, voortschrijdend inzicht of verbetering van procedures worden door het Bestuur verwerkt. Wijzigingen worden op de Isala website gepubliceerd.

Vragen of opmerkingen over dit document kunnen worden gericht aan het voor privacy eerstverantwoordelijke bestuurslid via email: privacy@zrzv-isala.nl

Versiebeheer:

0.1	20180406	Eerste conceptversie
0.2	20180406	Tekstuele aanpassingen, diverse correcties
0.3	20180407	Grondslag 'Overeenkomst' toegevoegd. Tekstuele aanpassingen.
0.4	20180426	Tekstuele aanpassingen, diverse correcties