Registratie van signalen rondom integriteit & AVG

februari 2024

Inleiding

Als bond kun je signalen over integriteitsschendingen krijgen. Bijvoorbeeld bij verenigingen, in de bondsorganisatie of in een topsportomgeving. In de Leidraad 'Zorgvuldig omgaan met signalen rondom integriteit' vind je meer informatie over het beoordelen en opvolgen van zulke signalen.

Goede registratie van signalen (en de opvolging ervan) is belangrijk. Het geeft inzicht in de tijdlijn, genomen besluiten en de onderbouwing ervan. Een dergelijk dossier moet voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Hoe zorg je daarvoor? Daar gaat deze leidraad over.

Let op! Deze leidraad helpt je op weg. Maar in de praktijk moet je bij elk signaal nog steeds een individuele afweging maken. Hoofdstuk 1 gaat in op de belangrijkste begrippen uit de AVG. Hoofdstuk 2 behandelt de algemene beginselen van de AVG. In hoofdstuk 3 geven we je praktische tips.

1. Belangrijke begrippen uit de AVG

De algemene verordening gegevensbescherming (AVG) is een privacywet, die geldt voor alle organisaties en zzp'ers die persoonsgegevens verwerken. Dit moet de privacy van mensen beschermen. Enkele belangrijke begrippen zijn:

- **Persoonsgegevens:** alle gegevens waarmee iemand geïdentificeerd kan worden. Bijvoorbeeld een naam, adres, telefoonnummer of pasfoto. En ook gegevens die naar iemand te herleiden zijn, zoals een identificatienummer.

- **Bijzondere persoonsgegevens:** gegevens die extra privacygevoelig zijn, en waarbij het meer impact heeft als deze gegevens worden verwerkt. Bijvoorbeeld iemands etnische afkomst, gezondheid, politieke voorkeuren of seksuele gerichtheid.

- **Strafrechtelijke persoonsgegevens:** gegevens over een strafblad, strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, en gegronde verdenkingen van strafbare feiten.

- **Verwerken van persoonsgegevens:** digitaal en/of hard copy gegevens verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen.

- **Grondslag:** een goede reden hebben voor het verwerken van persoonsgegevens. Volgens de AVG zijn er zes grondslagen voor gegevenswerking:
  - omdat de persoon om wie het gaat toestemming heeft gegeven
  - om een overeenkomst uit te voeren;
  - omdat je dit wettelijk verplicht bent;
  - om vitale belangen te beschermen;
  - om een taak van algemeen belang of openbaar gezag uit te oefenen;
  - vanwege een gerechtvaardigd belang van je organisatie.

2. Algemene beginselen uit de AVG

Voor de AVG is belangrijk dat je zorgvuldig omgaat met persoonsgegevens en goed kunt uitleggen waarom je gegevens verwerkt. De AVG gaat uit van zes algemene beginselen, waar iedere verwerking aan moet doen:

- rechtmatigheid en transparant werken;
- een duidelijk, welbepaalde doel hebben;
- minimalisatie van data;
- juistheid van data;
- bewaartermijnen hanteren;
- integriteit en veiligheid waarborgen.

Deze beginselen moeten terugkomen in alle stappen die je neemt en in de manier waarop je persoonsgegevens verwerkt. Dat geldt dus ook voor het dossier waarin je een signaal of melding verwerkt.

Rechtmatigheid en transparantie

De eerste eis is die van rechtmatigheid en transparantie. Rechtmatig betekent dat je voor de verwerking een grondslag hebt. Meestal zal dat *toestemming van de melder* zijn. Maar je kunt ook wijzen op het *gerechtvaardigd belang* om de sportomgeving veilig te houden. En op een *wettelijke plicht*, bijvoorbeeld de Arbeidsomstandighedenwet en de Wet bescherming klokkenluiders, als het signaal in je werkorganisatie speelt.

Daarnaast is transparantie over de manier waarop je persoonsgegevens verwerkt belangrijk. Zeker rondom integriteitssignalen en meldingen kun je niet alles delen. Vermeld daarom in een privacyverklaring en in meld- en onderzoeksprocedures welke persoonsgegevens je verwerkt, en met welk doel. Tip: maak er in de privacyverklaring een apart kopje van, dan is het extra zichtbaar.

Een privacyverklaring moet duidelijk en begrijpelijk zijn. Het is van belang om alledaagse taal te gebruiken. Daarnaast is het van belang om een goede structuur te gebruiken en per aparte verwerking toe te lichten op basis van welke grondslag er wordt verwerkt, welke categorieën persoonsgegevens voor welke doeleinden worden verwerkt en hoe lang de gegevens worden bewaard.

Tip: Check de privacyverklaring van jouw sportbond. Staat er iets in over de verwerkingen die jij verricht? Is duidelijk welke grondslagen de bond gebruikt, welke (soorten) persoonsgegevens verwerkt worden, waarom de bond dat doet, en hoe lang gegevens worden bewaard?

Duidelijk en welbepaald doel

Verwerking van persoonsgegevens moet een duidelijk doel hebben. En dat doel moet vooraf bepaald zijn. Bijvoorbeeld in een privacyverklaring. Ook mag je gegevens alleen voor het doel gebruiken, waarvoor je het verzamelde. En niet ineens voor een heel ander doel. Dat geldt voor alle persoonsgegevens in je dossier over het integriteitssignaal. Zorg er dus voor dat in de privacyverklaring goed vastligt dat je persoonsgegevens verzamelt om signalen en meldingen goed op te kunnen volgen.

Minimalisatie van data

Dataminimalisatie betekent dat je niet meer gegevens mag verwerken of gebruiken dan nodig is voor je doelen. Ook bij het verwerken van gegevens in een dossier over een integriteitssignaal moet je daar dus telkens op letten. In hoofdstuk 3 wordt dit verder praktisch uitgewerkt.

Juistheid van data

De AVG eist ook dat de persoonsgegevens die je verwerkt juist zijn. Daar moet de bond zelf voor zorgen. Check dus of alle persoonsgegevens die je krijgt correct zijn. Bijvoorbeeld door te controleren of een naam en lidmaatschapsnummer inderdaad bij elkaar horen. Blijf in het registreren van informatie zoveel mogelijk bij de feiten. Of geef duidelijk aan dat bepaalde informatie de mening of perceptie van een melder, getuige of beschuldigde is, en geen vaststaand feit.

Bewaartermijnen hanteren

Persoonsgegevens mogen niet langer dan nodig bewaard worden. Na het verstrijken van een bewaartermijn, moeten ze worden gewist. De bewaartermijn begint te lopen, zodra de melding is afgehandeld en het doel van de waarvoor je de persoonsgegevens verwerkte, is behaald. Voor integriteitsdossiers is op grond van de AVG geen concrete bewaartermijn vastgesteld. Dat verschilt per situatie. In H3 (onder ‘Afhandeling’) gaan we daar verder op in.

Integriteit en veiligheid

Persoonsgegevens moeten goed beveiligd zijn, zodat wordt gewaarborgd dat deze niet kunnen lekken of voor andere doelen gebruikt worden. Dat gaat dus over zorgvuldig omgaan met hard copy (geprinte) dossiers en documenten.

Maar ook over de beveiliging van digitale systemen. En over het waarborgen van geautoriseerd gebruik. In de praktijk betekent dit:

- sterke wachtwoorden en tweefactorauthenticatie op ICT-systemen;
- alleen toegang voor die personen waarvoor het absoluut noodzakelijk is;
- een geheimhoudingsverklaring (of gedragscode) voor degenen die toegang hebben;
- dossiers niet bespreken met personen die geen rol spelen bij de opvolging van de melding.

Let op! Een datalek is een inbreuk op de beveiliging, waardoor persoonsgegevens in verkeerde handen zijn gevallen of kwijt zijn geraakt. Ieder datalek moet intern worden geregistreerd. Vaak moeten datalekken ook bij de Autoriteit Persoonsgegevens en bij de betrokken personen gemeld worden.

Heb je zorgen hebt over integriteit en veiligheid, bespreek dit dan met de sportbond waarvoor je werkt. Indien nodig kan de sportbond de afdeling ICT van NOC*NSF inschakelen voor advies.

3. Praktische tips

De registratie van signalen over integriteit moet voldoen aan de AVG. Waar moet je dan op letten? Bij elke fase van opvolging geven we een aantal praktische tips.

Let op! Steeds meer sportbonden hebben een integriteitsmanager. Die is verantwoordelijk voor de registratie van signalen. In praktijk worden signalen ook geregistreerd door VCP'ers, en soms door andere functionarissen. Voor de leesbaarheid hebben we het in deze leidraad over de integriteitsmanager.

3.1 Ontvangst

Ontvangst van een signaal

Krijg je als bond een signaal van een mogelijke integriteitsschending? Meestal is dit een melding. Maar een signaal kan ook uit andere bronnen komen, zoals van collega's, een toezichthouder of uit de media. Dan maakt de integriteitsmanager (of de VCP) een dossier met een dossiernummer aan. Dit bevat:

- persoonsgegevens van de (eventuele) melder, beschuldigde en/of andere (direct) betrokkenen (bijvoorbeeld getuigen), zoals naam, lidmaatschapsnummer, de positie van deze personen (bijv. sporter, trainer, bestuurder) en de vereniging(en) waar het signaal speelt;
- beschrijving van de inhoud van het signaal: de feiten, omstandigheden en percepties van melders en betrokkenen, die te maken hebben met het signaal.

Wordt een melding niet in behandeling genomen, bijvoorbeeld omdat deze niet-ontvankelijk is? Dan wordt de melding niet in behandeling genomen. Informeer melder hierover, draag (indien van toepassing) het signaal over en verwijder de persoonsgegevens van de melder.

Persoonsgegevens melder

De melder moet uitdrukkelijk toestemming geven voor het verwerken van zijn/haar persoonsgegevens. Die toestemming is pas geldig als die:

- **vrij is gegeven:** dit houdt in dat iemand ook toestemming kan weigeren, zonder negatieve consequenties;
- **specifiek en geïnformeerd is:** de integriteitsmanager moet duidelijk aangeven waarom de persoonsgegevens worden verwerkt (welke gegevens en met welk doel);
- **ondubbelzinnig is:** er mag nooit twijfel bestaan over het feit dat toestemming is gegeven. Laat dit niet in het midden en maak daar een aantekening van;
- **ingetrokken mag worden:** dit mag te allen tijde.

Let op! Een privacyverklaring kan niet gebruikt worden om toestemming te vragen. Toestemming vragen moet altijd expliciet en apart gedaan worden.

Wordt een melding mondeling gedaan? Zorg dan dat de melding schriftelijk wordt vastgelegd, de melder een dossiernummer krijgt en een kopie van de melding krijgt voorgelegd. De melder kan deze dan aanvullen of bijstellen. Als de melder akkoord is met de inhoud van de melding, dan kan de melding, voorzien van dossiernummer en datum, worden opgeslagen.

Indien de melding via een vertrouwenspersoon is ontvangen, wordt de identiteit van de melder alleen met schriftelijke toestemming van de melder door de vertrouwenspersoon bekend gemaakt.

Persoonsgegevens van betrokkenen

Meestal worden in een signaal één of meerdere mensen beschuldigd. Ook kunnen getuigen of andere betrokkenen genoemd worden. Het is belangrijk dat mensen hierdoor niet onnodig beschadigd worden. Daarom moet zeer zorgvuldig omgegaan worden moet deze informatie. Alleen de integriteitsmanager, en de functionarissen die direct belast zijn met de opvolging van het signaal, mogen toegang hebben tot deze gegevens. Leg afspraken over toegang tot informatie bij voorkeur op voorhand vast.

Beschuldigden en getuigen die genoemd worden in een signaal, kunnen vooraf niet toestemming geven voor het verwerken van hun gegevens. Hoe ga je er als sportbond mee om als je ‘toestemming’ niet als grondslag kunt gebruiken?

- **Gewone persoonsgegevens** van betrokkenen mag je op basis van een *gerechtvaardigd belang* registreren. Als sportbond ben je immers verantwoordelijk voor de veiligheid van je leden en werknemers.
- **Bijzondere persoonsgegevens** verwerken is verboden, tenzij je je kan beroepen op een wettelijke uitzondering én het over het signaal gaat. Bijvoorbeeld bij signalen waar je werknemers mee te maken hebben. Dan moet je als werkgever namelijk de Arbeidsomstandighedenwet volgen, en bij een signaal over een onveilige werkomgeving ben je verplicht hier een dossier van te maken.
- **Strafrechtelijke persoonsgegevens** kunnen ook in een signaal naar voren komen. Meestal omdat je gegronde vermoedens van strafbare feiten krijgt. Sportbonden mogen deze persoonsgegevens niet registreren.

Tip! Bevat een signaal strafrechtelijke persoonsgegevens? Bijvoorbeeld een vermoeden van een strafrechtelijke overtreding? Registreer dan alleen de categorie van de integriteitsschending en leg de focus op zorg en professionele begeleiding van eventuele melders of slachtoffers. Verwijs direct door naar de politie. Die zal het signaal verder beoordelen en eventueel opvolging geven.

Een sportbond is verantwoordelijkheid voor de veiligheid van haar leden en werknemers. Dit kan betekenen dat een sportbond bij signalen over strafrechtelijke gedragingen zelf contact moet opnemen met de politie. Let op, dan nog mag je strafrechtelijke persoonsgegevens niet verwerken. Informeer de politie daarom mondeling of telefonisch. Registreer alleen de processtappen die je hebt gezet en de gegevens die je wel mag verwerken.

3.2 Opvolging

Registratie en onderzoeksdossier

Maak een onderscheid tussen registratie van een signaal en een eventueel onderzoeksdossier. Sla basisinformatie van een signaal (zoals naam, contactgegevens, geboortedatum, lidmaatschapsnummer) in een case information sheet. Registreer hier ook de processtappen die gezet worden. Ben je ook de partij die het integriteitsonderzoek doet? Bewaar dan in een gescheiden onderzoeksdossier de vertrouwelijke, inhoudelijke informatie, zoals gespreksverslagen, rapporten en andere informatie.

Alleen relevante informatie

De vuistregel is dat niet meer gegevens worden opgenomen dan noodzakelijk. Je stelt jezelf dus steeds de vraag wat relevante informatie is (‘*need to know*’) voor de afhandeling van de melding. In het dossier wordt informatie die niet direct relevant is (‘*nice to know*’) niet opgenomen. Vaak wordt de vraag gesteld wat relevante informatie is. Daar is geen pasklaar antwoord op te geven. Die afweging zal de integriteitsmanager in de praktijk steeds zelf opnieuw moeten maken. Zorg er wel voor dat je de gegevens registreert, die nodig zijn voor eventuele vervolgstappen. Zoals een tuchtrechtelijke behandeling of een arbeidsrechtelijke consequentie.

Persoonlijke werkaantekeningen

Persoonlijke werkaantekeningen worden niet in het dossier vastgelegd. Het zijn aantekeningen die dienen als geheugensteun voor de eigen gedachtevorming, dus om indrukken, vermoedens en vragen van degene die de aantekeningen maakt. Ook op aantekeningen zijn de eisen van voorzichtigheid, zorgvuldigheid en vertrouwelijkheid van toepassing. Vernietig persoonlijke aantekeningen direct nadat zij geen functie meer vervullen. Neem je persoonlijke aantekeningen wel in het dossier? Dan zijn ook de rechten van betrokkenen (bijvoorbeeld recht op inzage) daarop van toepassing.

Beoordeling van een signaal

Formeel is de directie of het bestuur van de sportbond verantwoordelijk voor de beoordeling en opvolging van signalen. Maak je als integriteitsmanager een schriftelijk advies of notitie, om over signalen met de directie te overleggen? Neem dan geen persoonsgegevens op, tenzij daar toestemming voor is gegeven door betrokkenen. Functionarissen die bij de opvolging van het signaal betrokken zijn, worden uitsluitend aangeduid met hun functie. Registreer het advies, de overwegingen en de vervolgstappen in het dossier.

Beschuldigde informeren

Een beschuldigde moeten worden geïnformeerd dat hij of zij onderdeel is van een signaal, en dat zijn of haar gegevens als onderdeel hiervan worden verwerkt. Maar een beschuldigde informeren kan pas als dit het onderzoeksbelang niet schaadt. Bijvoorbeeld omdat bewijsmateriaal eerst nog vergaard moet worden, getuigen niet beïnvloed mogen worden, of omdat de politie daar om vraagt. Informeer de beschuldigde dus zodra het kan. Deel dan in ieder geval ook een dossiernummer, zodat de beschuldigde gebruik kan maken van zijn of haar rechten onder AVG.

3.3 Afhandeling

Verzoek om inzage, correctie of verwijdering

Mensen hebben op grond van de AVG het recht om een verzoek te doen om inzage, correctie of verwijdering van persoonsgegevens. De sportbond kan hier dus een verzoek voor krijgen. Op zo'n verzoek moet je binnen een maand reageren. In principe moet een sportbond aan een verzoek voldoen. Bij integriteitszaken is dit echter lastig. Het gaat namelijk vaak juist om gevoelige informatie. En ook het onderzoeksbelang en de belangen van andere betrokkenen kunnen worden geschaad als een beschuldigde inzage krijgt in informatie. Op grond van de AVG (art. 23) mogen zulke verzoeken worden geweigerd, als dat nodig is om bijvoorbeeld strafbare feiten te voorkomen of op te sporen, of om de rechten en vrijheden van anderen te beschermen. Een (gedeeltelijke) weigering moet je wel goed kunnen onderbouwen, met een afweging waaruit blijkt dat het belang van de sportbond zwaarder weegt, of de rechten en vrijheden van anderen zwaarder wegen, dan het privacyrecht en de belangen van de beschuldigde. Ga daarom zorgvuldig om met zulke verzoeken en raadpleeg bij voorkeur een AVG-specialist.

Bewaartermijnen

De bewaartermijn begint te lopen wanneer het doel, waarvoor de persoonsgegevens worden verwerkt, is behaald. In dit geval omdat de melding is afgehandeld. Bijvoorbeeld omdat er onderzoek is gedaan, een sanctie is uitgesproken en deze straf (zoals een schorsing) ook is uitgevoerd. De bewaartermijn gaat pas in na aflopen van een sanctie of schorsing.

Soms kunnen dossiers direct worden vernietigd. Langer bewaren is dan niet nodig. Maar het kan noodzakelijk zijn gegevens langer te bewaren. Bijvoorbeeld als er concrete aanwijzingen zijn dat een juridische procedure (die verband houdt met de melding) wordt opstart of al loopt. Of omdat er een voorwaardelijke sanctie is uitgesproken. Bewaar een dossier in ieder geval zolang de mogelijkheid tot het starten van een juridische procedure nog mogelijk is. Denk aan de mogelijkheid om in beroep te gaan.

Er is op grond van de AVG geen concreet voorschrift voor bewaartermijnen van melddossiers. In de praktijk hanteren veel organisaties een bewaartermijn van gemiddeld vijf jaar. Als sportbond kun je zelf passende bewaartermijnen kiezen. Het beste leg je deze bewaartermijnen ook vast, bijvoorbeeld in je privacyreglement. Het Instituut Sportrechtspraak zal bewaartermijnen voor het tuchtrecht (onderzoeksdossiers, uitspraken) moeten bepalen, voor sportbonden die hierbij aangesloten zijn.

Let op! Zorg ervoor dat gegevens ook daadwerkelijk weggegooid worden als de bewaartermijn is verstreken. Weggooien wil zeggen daadwerkelijk en onomkeerbaar vernietigen. Gegevens horen dus niet in de (virtuele) prullenbak te komen. Vraag bij jouw organisatie na hoe vernietigen in de praktijk werkt.