

jongeren op gezond gewicht

Privacybeleid

Informatiebeveiliging, privacy en bescherming van persoonsgegevens

Inleiding

Jongeren Op Gezond Gewicht (JOGG) hecht veel waarde aan informatiebeveiliging, privacy en de bescherming van persoonsgegevens. Dit geldt ook voor de verwerking van persoonsgegevens van onze relaties. Daarom heeft JOGG de nodige stappen gezet om de gegevensverwerking nog veiliger te maken, de privacy te waarborgen en te voldoen aan de eisen die de wet hieraan stelt. In dit privacybeleid geeft JOGG heldere en transparante informatie over hoe zij omgaat met persoonsgegevens van haar betrokkenen (degenen van wie JOGG persoonsgegevens verwerkt).

Algemeen

JOGG doet er alles aan om de privacy te waarborgen en gaat daarom zorgvuldig om met persoonsgegevens. JOGG houdt zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming. Dit betekent onder andere dat:

- JOGG de persoonsgegevens verwerkt in overeenstemming met het doel waarvoor deze zijn verstrekt; deze doelen en type persoonsgegevens zijn beschreven in dit privacybeleid;
- verwerking van persoonsgegevens beperkt blijft tot enkel die gegevens die minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
- JOGG om toestemming vraagt als dat nodig is voor de verwerking van persoonsgegevens;
- er geen persoonsgegevens doorgegeven worden aan andere partijen, tenzij dit nodig is voor uitvoering van de doeleinden waarvoor ze zijn verstrekt;
- passende technische en organisatorische maatregelen zijn genomen zodat de beveiliging van de persoonsgegevens gewaarborgd is;
- JOGG op de hoogte is van de rechten inzake de verwerking van persoonsgegevens, JOGG hierop wijst en deze rechten respecteert.

Contactgegevens:

Klachten, vragen en opmerkingen over privacy kunnen gesteld worden bij:

Ilse Pardoen-Kwint

E: ilse.pardoen@jogg.nl

T: 070 219 22 65

Dit document geeft inzicht in en uitleg over hoe JOGG persoonsgegevens van betrokkenen beschermt, wat de rol van de medewerkers (iedereen die binnen de stichting een functie vervult, bestuurlijk, vanuit het secretariaat of als deelnemer van overleggen) hierin is en hoe de rechten van betrokkenen zijn geregeld.

In dit beleid worden dan ook de volgende onderwerpen behandeld:

1. Verwerken persoonsgegevens
2. Rechten van betrokkenen
3. Wat te doen bij een datalek
4. Proces uitvoering verwerkingen
5. Functionaris voor de Gegevensbescherming

1. Verwerken persoonsgegevens

Wat zijn persoonsgegevens

Op grond van de Algemene Verordening Gegevensbescherming (hierna te noemen AVG) is een persoonsgegeven 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van organisaties zijn geen persoonsgegevens.

jongeren op gezond gewicht

Voorbeelden van persoonsgegevens:

- NAW-gegevens van relaties, contactpersonen, telefoonnummers en e-mailadressen;
- ID/paspoort kopie, of BSN;
- Financiële gegevens (bijvoorbeeld gegevens met betrekking tot premies, loon of uitkeringen);

Wat wordt verstaan onder verwerken?

Onder verwerken van persoonsgegevens wordt verstaan: alle handelingen die een organisatie kan uitvoeren met betrekking tot persoonsgegevens, van verzamelen tot en met vernietigen. Dit is dus een zeer ruim begrip. Handelingen die er volgens de AVG in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Verwerking van persoonsgegevens van bestuur, partners

Persoonsgegevens van bestuur, commissie- en werkgroepleden en overige werknemers van de leden (bedrijven) waar JOGG contact mee heeft, worden door JOGG verwerkt ten behoeve van de volgende doelstellingen:

- Administratieve doeleinden;
- Communicatie over de werkzaamheden/activiteiten van de stichting en/of uitnodigingen;
- Het uitvoering geven aan of het uitvoeren van een opdracht;
- Het uitvoering geven aan de doelstellingen van de stichting;
- Inschrijvingen bij de Kamer van Koophandel

Grondslag voor deze persoonsgegevens is:

- De functie, taken en samenwerkingen die zij ten behoeve van de stichting vervullen;

Voor de bovenstaande doelstelling(en) kan JOGG de volgende persoonsgegevens vragen:

- Voornaam
- Tussenvoegsel
- Achternaam
- Geslacht
- Postcode
- Woonplaats
- (Zakelijk) Telefoonnummer
- (Zakelijk) E-mailadres
- (Zakelijke) functie
- Titels
- Geboorteplaats; geboortedatum; BSN-nummer; prive-adres*.

De persoonsgegevens worden door JOGG opgeslagen ten behoeve van bovengenoemde verwerking(en) voor de periode:

- Gedurende de periode dat de personen verbonden zijn met JOGG en daarna alleen in de financiële administratie voor maximaal 7 jaar.

* Deze gegevens worden opgevraagd voor inschrijvingen bij de Kamer van Koophandel en worden verder nergens opgeslagen.

jongeren op gezond gewicht

Verwerking van persoonsgegevens van nieuwsbrief abonnees

Persoonsgegevens van nieuwsbrief abonnees worden door JOGG verwerkt ten behoeve van de volgende doelstelling(en):

- Het informeren van de persoon d.m.v. nieuwsuitingen.

Grondslag voor deze persoonsgegevens is:

- Toestemming door het inschrijfformulier nieuwsbrief.

Voor de bovenstaande doelstelling(en) kan JOGG de volgende persoonsgegevens vragen:

- Voornaam
- Tussenvoegsel
- Achternaam
- E-mailadres

De persoonsgegevens worden door JOGG opgeslagen ten behoeve van bovengenoemde verwerking(en):

- Gedurende de periode dat men aangemeld is.

Verwerking van persoonsgegevens van prospect, stakeholder-/lobbycontacten en/of geïnteresseerde

Persoonsgegevens van potentiële partners, stakeholders-/lobbycontacten en/of geïnteresseerden worden door JOGG verwerkt ten behoeve van de volgende doelstelling(en):

- Informatieverstrekking in de vorm van nieuwsbrieven en/of gerichte contacten.

Grondslag voor deze persoonsgegevens is:

- Mondelinge of schriftelijke toestemming, afgifte visitekaartje en/of via koppeling op LinkedIn.

Voor de bovenstaande doelstelling(en) kan JOGG de volgende persoonsgegevens van u vragen:

- Voornaam
- Tussenvoegsel
- Achternaam
- Geslacht
- Telefoonnummer
- E-mailadres
- Zakelijke functie
- Zakelijk adres.

De persoonsgegevens worden door JOGG opgeslagen ten behoeve van bovengenoemde verwerking(en) voor de periode:

- Totdat de toestemming is ingetrokken.

Welke persoonsgegevens heeft JOGG

JOGG heeft veel verschillende soorten persoonsgegevens. JOGG heeft alleen persoonsgegevens voor zover die nodig zijn voor één van de hiervoor genoemde doeleinden. Is er geen noodzaak om persoonsgegevens te hebben, dan worden deze verwijderd. Er is een overzicht beschikbaar van de persoonsgegevens die worden verwerkt, het type verwerking, het doel van de verwerking en wie de persoonsgegevens verwerkt. Dit overzicht is op te vragen bij de contactpersoon die hierboven is genoemd.

Paspoorten / Identiteitskaarten

Voor het verwerken van persoonsgegevens moet een juridische grondslag bestaan. Dat geldt ook voor het overnemen, kopiëren of scannen van identiteitskaarten of paspoorten. Het is toegestaan om een

jongeren op gezond gewicht

kopie van een identiteitskaart of paspoort te maken indien er een wettelijke verplichting moet worden nagekomen of omdat er een overeenkomst uitgevoerd moet worden. Voor bijvoorbeeld de uitvoering van een partnerschap zijn betalingsgegevens nodig. De grondslag voor het verwerken van persoonsgegevens beperkt zich in deze gevallen tot het overnemen van de meest relevante gegevens. Het maken van een kopie van een identiteitskaart of paspoort is in geen van die gevallen nodig. Voor het inschrijven van toezichthouders/bestuurders bij de Kamer van Koophandel is wel een kopie identiteitskaart of paspoort nodig. Het is niet toegestaan om een kopie van de identiteitskaart of paspoort op te slaan. Zodra de inschrijving bij de Kamer van Koophandel is gebeurd, worden de kopieën identiteitskaart of paspoort verwijderd.

Met wie deelt JOGG persoonsgegevens

In principe deelt JOGG de gegevens niet met anderen. Mocht dit echter toch nodig zijn voor de uitvoering van de hiervoor beschreven doeleinden dan zijn hiervoor strenge regels van toepassing waaraan JOGG zich houdt. Zo zal er met de andere organisatie een verwerkersovereenkomst worden gesloten. In die overeenkomst worden afspraken gemaakt om de beveiliging van de persoonsgegevens te waarborgen. Voorbeelden van organisaties waarvan JOGG gebruik maakt zijn organisaties die de IT-systemen ontwerpen, onderhouden en verbeteren of bijvoorbeeld een accountantskantoor en salarisadministratiekantoor. Daarnaast zullen de persoonsgegevens worden verstrekt indien dit wettelijk verplicht en toegestaan is. Een voorbeeld hiervan is dat de politie in het kader van een onderzoek (persoons)gegevens opvraagt. In een dergelijk geval dient JOGG medewerking te verlenen en is JOGG dan ook verplicht deze gegevens af te geven. Ten slotte kan JOGG persoonsgegevens delen met derden indien daarvoor schriftelijk toestemming is gegeven.

JOGG verwerkt persoonsgegevens binnen de Europese Economische ruimte (EU landen, Noorwegen, IJsland en Liechtenstein) of naar of vanuit landen die een passend beschermingsniveau waarborgen in overeenstemming met de van toepassing zijn privacyregelgeving.

Hoe zorgt JOGG voor de persoonsgegevens

JOGG doet haar uiterste best om de privacy van persoonsgegevens die zij verwerkt te waarborgen. JOGG realiseert de privacybescherming en informatiebeveiliging door systematisch en continue beleid te bepalen, risico's te analyseren, maatregelen te nemen en toe te zien op de uitvoering.

JOGG draagt zorg voor passende technische en organisatorische maatregelen ter bescherming en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens.

JOGG maakt gebruik van een IT-omgeving in de cloud, die voldoende beschermd is. Deze omgeving is door verschillende factoren beschermt te weten:

- Er wordt een sterk wachtwoordenbeleid gehanteerd;
- Er is antivirus software (Symantec) op de laptops geïnstalleerd;
- Er is een Sophos firewall met Network Protection licentie en Web Protection licentie;

Binnen het pand waar JOGG zich bevindt zijn de volgende organisatorische maatregelen genomen:

- Bezoekers dienen zich te melden via de intercom bij de voordeur en vervolgens bij de balie van het secretariaat;
- Onbekende personen worden aangesproken;
- Medewerkers zijn geïnstrueerd hoe om te gaan met privacygegevens.

Alle medewerkers van JOGG dienen zich bewust te zijn van het feit dat zij regelmatig persoonsgegevens verwerken. Het is daarom van groot belang dat al deze medewerkers zorgdragen voor technische en organisatorische beveiligingsmaatregelen zoals:

- Alle medewerkers van JOGG mogen persoonsgegevens niet verder bekend maken dan voor de uitoefening van de functie noodzakelijk is. Dit geldt ook voor overige informatie waarvan men weet of redelijkerwijze kan vermoeden dat deze een vertrouwelijk karakter hebben;

jongeren op gezond gewicht

- Alle medewerkers hanteren een sterk wachtwoord voor hun devices waarop persoonsgegevens van relaties van JOGG staan. Wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door de medewerker zelf gebruikt te worden om toegang te krijgen tot de betreffende systemen. De medewerker geeft het wachtwoord dus niet aan derden of aan een collega;
- Alle medewerkers zijn geïnformeerd over het belang van de bescherming van persoonsgegevens;
- Het uitgangspunt is dat niet aan verzoeken om informatie over betrokkenen (personen op wie de privacygevoelige informatie betrekking heeft) wordt tegemoet gekomen. In uitzonderlijke gevallen kan informatie verstrekt worden aan derden, mits de identiteit van deze derde voldoende is vastgesteld (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie niet mogelijk is;
- Ook het vernietigen van vertrouwelijke (persoons)gegevens moet op een veilige manier plaats vinden. We stoppen vertrouwelijke gegevens nooit in de prullenbak.

2. Rechten van betrokkenen en indienen klacht

Iedere betrokkene (dat is degene op wie persoonsgegevens betrekking hebben) heeft een aantal rechten en JOGG is verplicht hieraan mee te werken. Zo mogen betrokkenen:

- Persoonsgegevens opvragen die JOGG over ze heeft;
- Uitleg vragen over waarom JOGG de gegevens over hen heeft;
- Toegang verlangen naar de persoonsgegevens;
- Hun persoonsgegevens laten bijwerken;
- Hun persoonsgegevens laten verwijderen;
- Hun persoonsgegevens laten overbrengen naar een andere relatie (dataportabiliteit);
- Inzicht krijgen in hoe JOGG voldoet aan de AVG en andere privacywetgevingen.

Als een betrokkene een verzoek doet om informatie, zijn de volgende regels van toepassing:

- Er wordt in geen enkel opzicht informatie over de betrokkene gedeeld met de verzoeker totdat is vastgesteld dat de verzoeker daadwerkelijk de betrokkene is. Betrokkene zal dan ook een legitimatiebewijs dienen te overleggen;
- Alleen gegevens die de betrokkene aan JOGG heeft geleverd of gegevens die voortvloeien uit het gedrag van de betrokkene mogen gedeeld worden;
- Op een verzoek zal zo snel mogelijk worden gereageerd maar uiterlijk binnen een maand na binnenkomst van het verzoek. Mocht dat niet lukken zal dit onderbouwd toegelicht worden aan de betrokkene;
- Er mogen geen kosten in rekening gebracht worden;
- Als het om een dataportabiliteitsverzoek gaat, hoeven alleen geautomatiseerde gegevens overgebracht te worden;
- Tenzij expliciet verzocht, is een verzoek van de betrokkene geen reden om de dienstverlening (tijdelijk) stop te zetten;
- Bij het versturen van de gegevens aan de betrokkene moet JOGG zorgen dat het transport adequaat beschermd is.

Indien JOGG persoonsgegevens verwerkt op basis van gegeven toestemming, dan heeft betrokkene altijd het recht deze toestemming in te trekken.

Een betrokkene kan het verzoek indienen bij JOGG.

Een betrokkene kan bezwaar maken tegen de gegevensverwerking. Dit bezwaar kan ingediend worden bij de contactpersoon op het gebied van het privacybeleid, zie contactgegevens hierboven. In het bezwaar dient de betrokkene een omschrijving te geven waartegen bezwaar wordt gemaakt. Er is een vast aanspreekpunt (zie contactgegevens hierboven) binnen JOGG hiervoor.

Ten slotte staat het een betrokkene vrij om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Dit is de toezichthoudende autoriteit op het gebied van privacy.

jongeren op gezond gewicht

Bewaartermijnen / verwijderen gegevens

JOGG bewaart de persoonsgegevens zo lang als nodig is voor het doel waarvoor de gegevens worden gebruikt en zo lang de wet JOGG verplicht om de gegevens te bewaren.

Hoe lang dat precies is, verschilt. In bijlage 1 is een overzicht van de bewaartermijnen opgenomen.

Zodra het bericht komt dat een persoon niet meer bij een organisatie werkzaam is, dan worden deze persoonsgegevens definitief verwijderd uit het relatiesysteem. Ook zullen alle persoonsgegevens die nu nog in de systemen zijn opgeslagen, maar waarvoor geen doel meer is, verwijderd worden.

3. Wat te doen bij een datalek

Hoewel alle medewerkers van JOGG dit beleid kennen, kan zich altijd een situatie voordoen dat er een beveiligingsincident of een datalek ontstaat. Een beveiligingsincident wordt gedefinieerd als: 'een inbreuk op de beveiliging, die gevolgen heeft voor de persoonsgegevens die zijn verwerkt. De maatregelen en de herstelmaatregelen die eventueel zijn getroffen, zijn niet voldoende om deze gevolgen geheel weg te nemen. Als gevolg hiervan kan een datalek ontstaan'. Een datalek wordt gedefinieerd als: 'een inbreuk op de beveiliging, die per ongeluk of op onrechtmatige wijze leidt tot onrechtmatige Verwerking of de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte Persoonsgegevens, als bedoeld in artikel 13 jo. artikel 34a Wbp en artikel 4 lid 12 AVG'.

Als een medewerker te maken krijgt met een beveiligingsincident en/of datalek dient dit direct gemeld te worden bij het aanspreekpunt privacybeleid, Ilse Pardoën-Kwint. Tevens dient dit direct gemeld te worden bij de verantwoordelijke van het Management Team, Marjon Bachra. Ook bij twijfel dient er contact opgenomen te worden met het aanspreekpunt privacybeleid. Deze medewerker zal onderzoeken of er daadwerkelijk sprake is van een beveiligingsincident en/of datalek en welke stappen ondernomen moeten worden. Om adequaat te kunnen reageren bij een beveiligingsincident is het belangrijk dat verlies of diefstal van een device onmiddellijk, maar binnen 24 uur, kenbaar wordt gemaakt aan het aanspreekpunt privacybeleid.

Ernstige datalekken worden overeenkomstig de regelgeving gemeld bij de Autoriteit Persoonsgegevens.

Versturen e-mails

Er is bijvoorbeeld al sprake van een datalek indien e-mails aan een groep personen vanuit het 'aan-veld' worden verstuurd. E-mails worden daarom zoveel als mogelijk in de BCC verstuurd. Dat geldt in ieder geval voor e-mails die naar groepen worden verstuurd waarvan de deelnemers elkaar niet kennen. E-mails aan bestuur en vaste groepen mogen wel gewoon via het 'aan-veld' worden verstuurd.

4. Proces uitvoering verwerkingen

De verwerkingen van persoonsgegevens die JOGG voor invoering van de AVG al deed, zijn beoordeeld en waar nodig aan de AVG aangepast. Bij het opstellen van de verwerkingen en de grondslag wordt beoordeeld of JOGG niet meer gegevens vraagt en/of ontvangt dan die nodig zijn voor de verwerkingen.

Bij het ontwikkelen van producten en diensten zorgt JOGG ervoor dat wordt voldaan aan het informatiebeveiligingsbeleid en de AVG.

5. Functionaris voor de Gegevensbescherming (FG)

Kijkend naar de aard van de werkzaamheden van JOGG, de omvang van de verwerking van persoonsgegevens en de criteria voor het aanstellen van een FG vanuit de Autoriteit Persoonsgegevens ziet JOGG op dit moment geen noodzaak om een FG aan te stellen.

jongeren op gezond gewicht

Tot slot

JOGG heeft een open cultuur waarbij iedereen elkaar aanspreekt op het eigen gedrag rondom de bescherming van persoonsgegevens en daarmee van elkaar leert. Communicatie, openheid en toetsing zijn belangrijk om het beleid te realiseren.

jongeren op gezond gewicht

Bijlage 1: bewaartermijnen

	Document	Wettelijke bewaartermijn	Richtlijn bewaartermijn	Persoonsgegevens
FINANCIEEL	Jaarrekening, accountantsverklaring	10 jaar (volgens subsidieregels)	Oneindig	Niet aanwezig
	Facturen (inkomend en uitgaand)	10 jaar (volgens subsidieregels)	10 jaar, na afsluiten boekjaar	Naam contactpersoon en geslacht
	Grootboek, debiteuren/crediteurenadministratie, in- en verkoopadministratie, voorraad- en loonadministratie (Afas)	10 jaar (volgens subsidieregels)	10 jaar, na afsluiten boekjaar	Naam, adres, woonplaats, rekeningnummer, geslacht, telefoonnummer en emailadres
	Klantgegevens	10 jaar (volgens subsidieregels)	10 jaar, na start relatie	Naam, mailadres, functie, adres en telefoonnummer contactpersoon
	Administratie subsidieaanvraag	Conform subsidievoorwaarden		
	Belastingaangifte (omzet- en vennootschapsbelasting)	10 jaar (volgens subsidieregels)	10 jaar, na afsluiten boekjaar	Niet aanwezig
	Rapport controle belastingdienst	10 jaar (volgens subsidieregels)	Oneindig	Niet aanwezig
VERENIGING EN BESTUUR	Uittreksel KvK, statuten, statutenwijzigingen		Oneindig Inschrijfformulier wordt verniegid zodra de inschrijving is verwerkt	Naam, adres, woonplaats, geslacht, geboortedatum en geboorteplaats, id-nummer (statuten)
	Bestuurs- en ledenstukken		Oneindig	Naam
	Financiën (jaarrekeningen, jaarverslag begrotingen)		Oneindig	In jaarverslag staat naam bestuurslid. In overige stukken geen gegevens.
	Relatiebeheersysteem		Niet langer bewaren dan de persoon werkzaam is bij de organisatie en/of deze organisatie	Naam, telefoonnummer, emailadres, geslacht, geboortedatum, adres, woonplaats, functie.

jongeren op gezond gewicht

			een overeenkomst heeft.	
	Commissie- of werkgroepverslagen en documenten		7 jaar	Namen aanwezig
COMMISSIES / WERKGROEP EN/	Administratie subsidies	Conform subsidievoorwaarden		
	Vertegenwoordiging in externe organisaties		Zo lang er deelname aan de organisatie is	Naam, mailadres, geslacht