Informatiebeveiliging, privacy en bescherming van persoonsgegevens

Inleiding

FEDA hecht veel waarde aan informatiebeveiliging, privacy en de bescherming van persoonsgegevens. Dit geldt ook voor de verwerking van persoonsgegevens van onze klanten. Daarom heeft FEDA 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 FEDA heldere en transparante informatie over hoe FEDA omgaat met persoonsgegevens van haar betrokkenen (degenen van wie FEDA persoonsgegevens verwerkt).

Algemeen

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

- FEDA de persoonsgegevens verwerkt in overeenstemming met het doel waarvoor deze zijn verstrekt; deze doelen en type persoonsgegevens zijn beschreven in dit privacy beleid;
- verwerking van persoonsgegevens beperkt blijft tot enkel die gegevens die minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
- FEDA 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;
- FEDA op de hoogte is van de rechten inzake de verwerking van persoonsgegevens, FEDA hierop wijst en deze rechten respecteert.

Contactgegevens

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

FEDA
Stephensonweg 14
4207 HB Gorinchem
info@feda.nl
Telefoonnummer: 0183- 822 992

Dit document geeft inzicht in en uitleg over hoe FEDA persoonsgegevens van betrokkenen beschermt, wat de rol van de functionarissen (iedereen die binnen de vereniging/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. Rechten van betrokkenen en klachten
5. Proces uitvoering verwerkingen
6. 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.

Voorbeelden van persoonsgegevens:

- NAW-gegevens van relaties, contactpersonen of leden, telefoonnummers en e-mailadressen
- ID/paspoort kopie, of BSN
- Financiële gegevens (bankrekeningnummer)
- Lidmaatschapsgegevens van verenigingen, stichtingen en publiekrechtelijke beroepsorganisaties

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, leden, aangesloten werkgevers/werknemers

Persoonsgegevens van bestuur, werkgroepleden, leden, aangesloten werkgevers worden door "FEDA" verwerkt ten behoeve van de volgende doelstelling(en):

- Administratieve doeleinden;
- Communicatie over de opdracht en/of uitnodigingen;
- Het uitvoering geven aan of het uitgeven van een opdracht;
- Het uitvoering geven aan de doelstellingen van de vereniging / stichting;
- Verkopen, betalen en leveren van producten uit de webshop.

Grondslag voor deze persoonsgegevens is:

- De overeengekomen opdracht;

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

- Voornaam;
- Tussenvoegsel;
- Achternaam;
- Postcode;
- Woonplaats;
- (Zakelijk) Telefoonnummer;
- (Zakelijk) E-mailadres;
- Geslacht;
- Geboortedatum;

- Geboorteplaats;
- Nationaliteit;
- Titels;
- Kopie ID-bewijs;
- Rekeningnummer;
- BSN-nummer;
- Functie.

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

- Gedurende het lidmaatschap met "FEDA" / aansluiting bij "FEDA" en daarna alleen in de financiële administratie voor maximaal 7 jaar.

Verwerking van persoonsgegevens van nieuwsbrief abonnees en mailings
Persoonsgegevens van Nieuwsbrief abonnees worden door "FEDA" verwerkt ten behoeve van de volgende doelstelling(en):

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

Grondslag voor deze persoonsgegevens is:

- Toestemming door het inschrijfformulier nieuwsbrief; of
- Werknemer bij een FEDA-lid en/of
- Lid van een werkgroep of een commissie/bestuur

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

- Voornaam;
- Tussenvoegsel;
- Achternaam;
- (Zakelijk) Telefoonnummer;
- (Zakelijk) E-mailadres;
- Geslacht;
- Titels;
- Rekeningnummer;
- BSN-nummer;
- Functie.

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

- Gedurende de periode dat men aangemeld is
- Of werkzaam is bij het bedrijf dat lid is van FEDA.

Verwerking van persoonsgegevens van prospect, stakeholder-/lobbycontacten en/of geïnteresseerde
Persoonsgegevens van prospect, stakeholder-/lobbycontacten en/of geïnteresseerde worden door "FEDA" verwerkt ten behoeve van de volgende doelstelling(en):

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

Grondslag voor deze persoonsgegevens is:

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

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

- Voornaam;
- Tussenvoegsel;
- Achternaam;
- Telefoonnummer;
- E-mailadres;
- Functie.

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

Totdat de toestemming is ingetrokken.

Welke persoonsgegevens heeft FEDA
FEDA heeft veel verschillende soorten persoonsgegevens. FEDA 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 het secretariaat.

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 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 lidmaatschap 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 bestuurders bij de Kamer van Koophandel is wel een kopie identiteitskaart of paspoort nodig. FEDA adviseert het gebruik van de KopieID app van het Ministerie van Buitenlandse Zaken. 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 FEDA *persoonsgegevens*
In principe deelt FEDA 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 FEDA 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 FEDA gebruik maakt zijn organisaties die de IT-systemen ontwerpen, onderhouden en verbeteren of een accountantskantoor. 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 FEDA medewerking te verlenen en is FEDA dan ook verplicht deze gegevens af te geven. Ten slotte kan FEDA persoonsgegevens delen met derden indien daarvoor schriftelijk toestemming is gegeven.

FEDA 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 FEDA voor de persoonsgegevens
FEDA doet haar uiterste best om de persoonsgegevens die zij verwerkt te waarborgen. FEDA 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.

FEDA draagt zorg voor passende technische en organisatorische maatregelen ter bescherming en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens.
FEDA maakt gebruik maken de omgeving van Atriumgroep. Deze cloud omgeving is door verschillende factoren beschermt te weten:

- Er wordt een sterk wachtwoorden beleid gehanteerd.
- Multifactor authenticatie voor het toegang krijgen tot de Citrix Desktop via het publieke web portaal.
- Alle sites worden gepubliceerd door een Netscaler met daarop geactiveerde beveiligings features zoals web application firewall.
- Netwerk segmentering is toegepast binnen de cloud omgeving.
- Maandelijkse PEN testen op externe pagina`s die vanuit de datacenter locatie worden gepubliceerd.
- Op alle servers staat f-secure antivirus met deep guard functionaliteit enabled.
- De cloud omgeving wordt beschermd door twee Next Generation Firewalls met Unified Threat Management functionality (UTM).
- De infrastructuur (on site) is fysiek beveiligd.

Binnen het pand waarin het secretariaat van FEDA zich bevindt zijn de volgende organisatorische maatregelen genomen:
- Bezoekers dienen zich te melden bij de receptie;
- Onbekende personen worden aangesproken
- Functionarissen zijn geïnstrueerd hoe om te gaan met privacygegevens
- Het pand is voorzien van een beveiligingssysteem en wordt 's-avonds afgesloten door een daartoe bevoegde particulier beveiliger.

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

- Alle functionarissen van FEDA 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.
- Alle functionarissen hanteren een sterk wachtwoord voor hun devices waarop persoonsgegevens van relaties van FEDA staan. Wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door de functionaris zelf gebruikt te worden om toegang te krijgen tot de betreffende systemen. De functionaris geeft het wachtwoord dus niet aan derden of aan een collega.
- Alle functionarissen 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. Stop vertrouwelijke gegevens nooit in de prullenbak.

2. Rechten van betrokkenen en indienen klacht

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

- Persoonsgegevens opvragen die het bedrijf over ze heeft;
- Uitleg vragen over waarom de organisatie de gegevens over hen heeft;
- Toegang verlangen naar de persoonsgegevens;
- Hun persoonsgegevens bijwerken of laten bijwerken;
- Hun persoonsgegevens laten verwijderen;
- Hun persoonsgegevens laten overbrengen naar een andere relatie (dataportabiliteit);
- Inzicht krijgen in hoe het bedrijf 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 FEDA 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 de organisatie zorgen dat het transport adequaat beschermd is.

Indien FEDA 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 FEDA. De betrokkene kan het verzoek ook rechtstreeks bij het privacyteam van Atriumgroep indienen. In beide gevallen zal het privacyteam van Atriumgroep het verzoek behandelen.

Een betrokkene kan bezwaar maken tegen de gegevensverwerking. Dit bezwaar kan ingediend worden bij FEDA of rechtstreeks bij het privacyteam van Atriumgroep. In beide gevallan zal het privacyteam het bezwaar behandelen. In het bezwaar dient de betrokkene een omschrijving te geven waartegen bezwaar wordt gemaakt.

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.

Bewaartermijnen / verwijderen gegevens
FEDA bewaart de persoonsgegevens zo lang als nodig is voor het doel waarvoor de gegevens worden gebruikt en zo lang de wet FEDA verplicht om de gegevens te bewaren. Hoe lang dat precies is, verschilt. In bijlage 1 is een overzicht van de bewaartermijnen opgenomen.

Naast alle gegevens die zijn opgenomen in stukken die zijn genoemd in de bijlage, zijn er ook persoonsgegevens in het relatiesysteem opgenomen onder de organisaties en onder personen.
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 functionarissen van FEDA 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 functionaris te maken krijgt met een beveiligingsincident en/of datalek dient dit direct gemeld te worden bij het privacyteam van Atriumgroep via de e-mail privacy@Atriumgroep.nl. Tevens dient er direct telefonisch contact opgenomen te worden met één van de leden van het privacyteam. Ook bij twijfel dient er contact opgenomen te worden met het privacyteam. Het privacyteam zal onderzoeken of er daadwerkelijk sprake is van een beveiligingsincicent en/of datalek en welke stappen ondernomen moeten worden. Hiervoor is door het privacyteam stappenplan datalek opgesteld. Dit stappenplan kan bij Atriumgroep worden opgevraagd. 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 privacyteam.

Versturen e-mails
Er is bijvoorbeeld sprake van een datalek indien e-mails aan een groep personen vanuit het 'aan-veld' worden verstuurd. E-mails worden daarom zoveel 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, werkgroepen mogen wel gewoon via het 'aan-veld' worden verstuurd.

4. Proces uitvoering verwerkingen

De verwerkingen van persoonsgegevens die FEDA 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 FEDA niet meer gegevens vraagt en/of ontvangt dan die nodig zijn voor de verwerkingen.

Bij het ontwikkelen van producten en diensten zorgt FEDA ervoor dat wordt voldaan aan het informatiebeveiligingsbeleid en de AVG. Nadat FEDA alles in kaart heeft gebracht, bepaalt FEDA of een Privacy Impact Assessment (PIA) verplicht is en/of dat toegevoegde waarde heeft. Als dat het geval is, dan voert FEDA een PIA uit.

5. Functionaris voor de Gegevensbescherming (FG)

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

Tot slot

FEDA 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.

Bijlage 1: bewaartermijnen

	Document	Wettelijke bewaartermijn	Richtlijn bewaartermijn	persoonsgegevens
FINANCIEEL	Jaarrekening, accountantsverklaring	7 jaar	Oneindig	Niet aanwezig
	Facturen (inkomend en uitgaand)	7 jaar	7 jaar, na afsluiten boekjaar	Naam contactpersoon en geslacht, e-mailadres, adres, woonplaats, rekeningnummer
	Grootboek, debiteuren/crediteurenadministratie, in- en verkoopadministratie, voorraad- en loonadministratie (Elvy, Exact, Caseware, Docs, Qics)	7 jaar	7 jaar, na afsluiten boekjaar	Naam, adres, woonplaats, rekeningnummer, geslacht, telefoonnummer en emailadres
	Klantgegevens	7 jaar	7 jaar, na start relatie	Naam contactpersoon?
	Administratie subsidieaanvraag	Conform subsidievoorwaarden		
	Belastingaangifte (omzet- en vennootschapsbelasting)	7 jaar	7 jaar, na afsluiten boekjaar	Niet aanwezig
	Rapport controle belastingdienst	7 jaar	Oneindig	Niet aanwezig
VERENIGING EN BESTUUR	Uittreksel KvK, statuten, statutenwijzigingen		Oneindig Inschrijfformulier vernietigen 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

	Ledenadministratie stichting of vereniging	10 jaar	10 jaar (het enige dat je oneindig wilt bewaren zijn de namen van de bedrijven die ooit allemaal lid zijn geweest. De gehele administratie lijkt ons niet zinnig)	Naam, telefoonnummer, emailadres, geslacht, geboortedatum, adres, woonplaats
	Relatiebeheersysteem		Niet langer bewaren dan de persoon werkzaam is bij de organisatie en/of deze organisatie een overeenkomst heeft.	Naam, telefooonnummer, emailadres, geslacht, geboortedatum, adres, woonplaats
	Commissies t.b.v. cao		Oneindig	Namen aanwezigen
	Commissie- of werkgroepverslagen en documenten		7 jaar	Namen aanwezigen
	Geschillencommissies, beroepscommissies		oneindig	Namen partijen, namen aanwezigen. Partijen: naam, adres, woonplaats, email, geslacht, lidmaatschap vakbond, salarisgegevens, telefoon
	Administratie subsidies	Conform subsidievoorwaarden		

EXTERNE VERTEGENWOORDIGINGEN	Vertegenwoordiging in externe organisaties		Zo lang er deelname aan de organisatie is	Naam, mailadres, geslacht