



AVG en Opt-in beheer

Handleiding Smart CRM & Marketing Platform

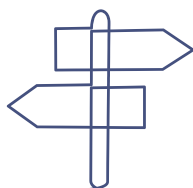
Versie: 1.6 | Classificatie: Vertrouwelijk

Inhoudsopgave

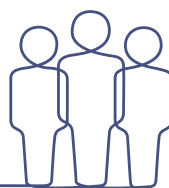
Introductie	3
1 De AVG en privacy van personen	4
2 Hoe ga je om met AVG binnen het SMP?.....	5
2.1 Toestemmingen: Opt-in Opt-outs	5
2.2 Opt-in types beheren.....	6
2.2.1 Opt-in soorten	6
2.2.2 Zoekvraag automatisch toekennen zachte opt-ins	7
2.2.3 Automatisch zachte opt-outs toekennen	9
2.3 Voorkeuren in de klantkaart.....	9
2.3.1 Handmatig in-/ uitschrijven van en persoon.....	9
2.3.2 Persoon volledig uitschrijven	10
2.4 Anonimiseren.....	11
2.5 Bewaartermijnen en doorlopend anonimiseren	12
2.6 Bouncers.....	13
2.7 PDF met persoonsgegevens.....	14
2.8 Zoekvraag maken voor een nieuwsbrief.....	14
3 Waar moet je zelf op letten?	16
4 Begrippenlijst	17



Inzicht



Strategie



Organisatie



Technologie

Introductie

Deze handleiding helpt je om op een juiste en zorgvuldige manier te werken binnen de kaders van de Algemene Verordening Gegevensbescherming (AVG), in combinatie met het gebruik van het Smart CRM & Marketing Platform (SMP). Je vindt in deze handleiding praktische uitleg en richtlijnen over hoe je persoonsgegevens veilig en transparant verwerkt binnen het platform.

De volgende onderwerpen komen onder andere aan bod:

- De AVG en de privacy van personen
- Opt-in beheer
 - Verschillende opt-in types
 - Harde en zachte opt-ins
- Aan- en afmeldprocessen
 - Handmatig aanmelden en afmelden
 - Volledig afmelden
- Privacy functionaliteiten binnen SMP
 - Anonimiseren van persoonsgegevens
 - Bewaartermijnen en doorlopend anonimiseren
- Rechten van betrokkenen
 - Inzage in persoonsgegevens
- Bounces (onbestelbare e-mails)

Met deze handleiding ben je verzekerd van een juiste toepassing van de AVG binnen het Smart CRM & Marketing Platform.

1 De AVG en privacy van personen

De Algemene Verordening Gegevensbescherming (AVG) is de privacywetgeving die sinds 25 mei 2018 van kracht is in de hele Europese Unie. De AVG verplicht organisaties om zorgvuldig om te gaan met persoonsgegevens en hier transparant over te zijn richting betrokkenen.

Concreet betekent dit dat organisaties duidelijk moeten vastleggen:

- Waarom zij persoonsgegevens verzamelen (doel van de verwerking).
- Waarvoor zij deze gegevens gebruiken (de verwerkingsdoeleinden).
- Hoe lang de gegevens worden bewaard (bewaartermijn).

Deze verplichtingen leiden tot meer en betere documentatie van de manier waarop persoonsgegevens worden verzameld, verwerkt en bewaard.

Privacy van personen

De AVG versterkt het recht op privacy door personen meer controle te geven over hun eigen persoonsgegevens. Personen hebben onder de AVG onder andere de volgende rechten:

- Het recht om **toestemming op een eenvoudige manier te geven, aan te passen of in te trekken**.
- Het recht op **inzage** in hun gegevens: zij mogen opvragen welke persoonsgegevens een organisatie van hen heeft en wat daarmee gebeurt.
- Het recht om **vergeten te worden**: zij kunnen organisaties verzoeken hun persoonsgegevens te verwijderen.
- Het recht op **overdraagbaarheid van gegevens**: zij kunnen hun gegevens opvragen en overdragen naar een andere dienstverlener.

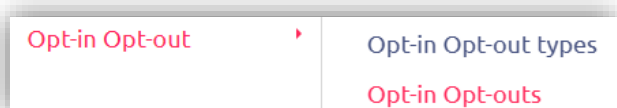
Deze rechten gelden niet alleen richting jouw organisatie, maar ook richting alle partijen waarmee je persoonsgegevens deelt. Daarom is het verplicht om met alle verwerkers van persoonsgegevens een **verwerkersovereenkomst** af te sluiten. Hierin worden de afspraken vastgelegd over de omgang met de gegevens, zodat ook deze partijen zich houden aan de regels van de AVG.

2 Hoe ga je om met AVG binnen het SMP?

Binnen het SMP zijn diverse functionaliteiten beschikbaar die je ondersteunen bij het naleven van de AVG. Daarnaast zijn er enkele belangrijke aandachtspunten om rekening mee te houden. In dit hoofdstuk bespreken we deze onderdelen stap voor stap.

2.1 Toestemmingen: Opt-in Opt-outs

In het SMP worden de opt-ins en opt-outs van relaties centraal beheerd. Deze zijn te vinden via het menu item **'Relaties'**, onder het submenu **'Opt-in Opt-out'**. Hier klik je op **'Opt-in en Opt-outs'** om in een overzichtelijke tabel te komen waarin van alle personen in het SMP de gegeven toestemmingen (opt-ins) en afmeldingen (opt-outs) worden bijgehouden. Ook de volledige historie van wijzigingen wordt hier vastgelegd.



Bij iedere wijziging wordt er automatisch een nieuwe registratie (record) aangemaakt. Per registratie wordt de onderstaande informatie opgeslagen, zodat op een volledig AVG-conforme manier wordt gewerkt:

- **Id:** Elke registratie (record) krijgt een uniek Id
- **Datum:** De datum en het tijdstip waarop de opt-in of opt-out is vastgelegd
- **Persoon:** De persoon die de opt-in of opt-out heeft gegeven
- **Kanaal:** Het kanaal of de methode waarmee de toestemming is vastgelegd. Denk aan het voorkeurencentrum, een online webformulier, de eigen website of handmatige invoer.
- **Opt-in:** Aangevinkt (ja) betekent een opt-in; leeg (nee) betekent een opt-out.
- **Type:** Het type opt-in, bijvoorbeeld: toestemming voor de nieuwsbrief, servicemail of vrienden-nieuwsbrief.
- **Omschrijving:** De tekst die is gecommuniceerd bij het geven van de opt-in of opt-out. Vaak betreft dit de labeltekst zoals deze op een formulier of website is weergegeven.
- **Zacht afgegeven:** Wanneer de opt-in of opt-out 'zacht' is afgegeven, wordt dit veld aangevinkt.
Een zacht gegeven opt-in wordt altijd overschreven indien er ook een hard gegeven opt-in of opt-out aanwezig is voor hetzelfde type opt-in. Zacht afgegeven opt-ins worden in dat geval genegeerd.

- **Contactmoment:** Wanneer iemand via een mailing, verzonden vanuit het SMP, een opt-in of opt-out geeft, wordt hier geregistreerd vanuit welk contactmoment dit heeft plaatsgevonden.

2.2 Opt-in types beheren

Om de voorkeuren van relaties goed te beheren in het SMP en transparant te zijn naar relaties heb je de mogelijkheid om verschillende opt-in types aan te maken. Een aantal veelvoorkomende voorbeelden hiervan zijn:

- Nieuwsbrief
- Servicemail
- Profileren

In het SMP beheer je de opt-in types vanuit de Opt-in Opt-out type tabel. Deze tabel is te vinden onder het menu item 'Relaties', onder het submenu 'Opt-in Opt-out'.



Afhankelijk van jouw gebruikersgroep heb je hier de mogelijkheid om de beschikbare opt-in types in te zien of, te wijzigen en/of nieuwe toe te voegen. Bij het inrichten van een opt-in type kies je onder andere een label zoals hij zichtbaar is voor relaties, een omschrijving welke de lading dekt en voor welk kanaal hij geldt. In onderstaande screenshot is een weergave te zien van alle te bepalen velden, de tooltips onder het vraagteken geven de benodigde instructie over de exacte werking van de velden.

2.2.1 Opt-in soorten

Belangrijk bij het inrichten van een opt-in type is de keuze voor het soort opt-in (het veld: Soort).

Er zijn hierbij twee opties om uit te kiezen:

1. **Harde opt-in:** Dit betekent dat een relatie actief en expliciet toestemming heeft gegeven voor het ontvangen van bijvoorbeeld marketingberichten of nieuwsbrieven.

Kenmerken:

- De relatie heeft zelf een vinkje gezet of expliciet 'ja' gezegd
- Vaak vastgelegd via een formulier of binnen een aanmeldproces
- Goed gedocumenteerd en makkelijk te bewijzen
- Past bij privacywetgeving (zoals AVG / GDPR) voor commerciële communicatie

2. **Zachte opt-in:** Een zachte opt-in betekent er niet actief toestemming is gegeven, maar je mag ze toch benaderen, omdat er een bestaande relatie is of omdat het logisch voortvloeit uit de situatie (bijvoorbeeld een aankoop of dienst).

Kenmerken:

- Gebaseerd op een klantrelatie of een logische verwachting (bijvoorbeeld bij serviceberichten).
- Vaak gebruikt voor: Serviceberichten (zoals bevestigingen, storingsmeldingen, updates)
- Commerciële berichten naar bestaande klanten, mits afmeldmogelijkheid wordt geboden.
- Toegestaan onder voorwaarden van de privacywet, zolang een opt-out mogelijk is.

2.2.2 Zoekvraag automatisch toekennen zachte opt-ins

Indien gekozen is voor optie 2: 'Zachte opt-in' dan krijg je de mogelijkheid om deze automatisch toe te laten kennen. Er verschijnen hiervoor een aantal nieuwe velden in de sectie 'Geavanceerde instellingen'.



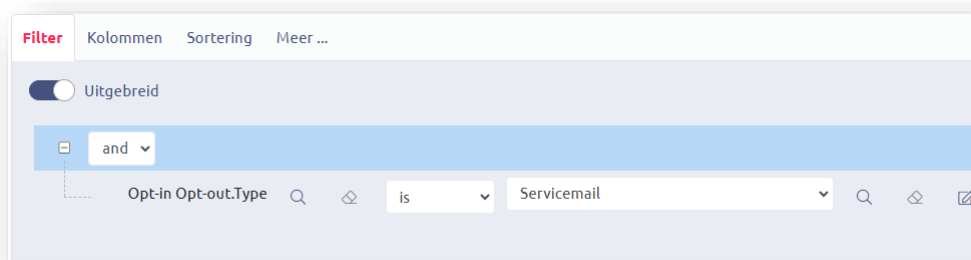
Geavanceerde instellingen	
Tonen op formulier	☒
Aanpasbaar	☒
Tonen aan iedereen	☒
Volgorde	2
Tonen op website	☐
Automatisch opt-ins toevoegen	☒
Selectie voor opt-ins	SCAVDK - 20221228 - Zachte opt-ins - Servicemail
Automatisch opt-outs toevoegen	☐
Selectie voor opt-outs	

Voor het automatisch toekennen van zachte opt-ins is een zoekvraag nodig.

Of het automatisch toekennen van opt-ins wenselijk is voor jouw organisatie kan verschillen per situatie. In dit voorbeeld willen we een servicemail opt-in standaard toekennen aan alle personen. In dit geval is het belangrijk om in de zoekvraag personen uit te sluiten die al een record hebben voor dit opt-in type in de Opt-in Opt-out tabel.

Deze zoekvraag en subzoekvraag (voor de uitsluiting) richt je als volgt in:

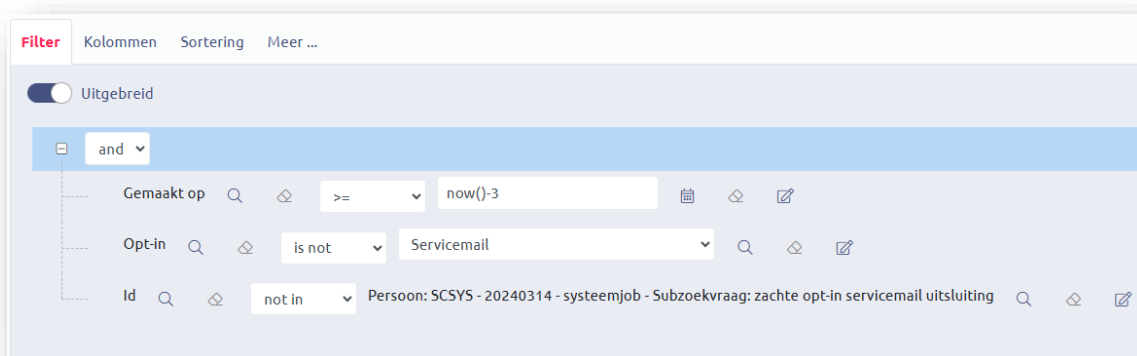
1. Selecteer door middel van een zoekvraag op de Persontabel iedereen die een record heeft met dit opt-in type. Zorg in het tabblad kolommen dat alleen de kolom 'id' zichtbaar is.



Sla deze zoekvraag herkenbaar op om te gebruiken als subzoekvraag.

2. Maak een nieuwe zoekvraag in de Persontabel en selecteer hierin alle personen die:
 - a. Gemaakt zijn in de laatste 3 dagen ('now()-3')
 - b. Het opt-in type nog niet hebben ('is not Servicemail').
 - c. Voeg de uitsluiting toe, verwijst naar de subzoekvraag uit stap 1 ('not in').

Sla deze zoekvraag nu herkenbaar op.



Kies tot slot bij het betreffende opt-in type in de 'Opt-in Opt-out type tabel' in het veld 'Selectie voor opt-ins' de zoekvraag uit stap 2.

2.2.3 Automatisch zachte opt-outs toekennen

Naast het automatisch toekennen van opt-ins is het ook mogelijk om automatisch zachte opt-outs toe te kennen. De functionaliteit werkt hetzelfde als het toekennen van automatische opt-ins.

2.3 Voorkeuren in de klantkaart

De klantkaart bevat alle gegevens van een persoon. De gegevens zijn opgedeeld in een aantal tabbladen. In het tabblad 'Voorkeuren' is alle informatie te vinden met betrekking tot actieve opt-ins, opt-in historie en interesses.

Tag	Bron
Genre: Zang	Persoon
Genre: Cabaret	Persoon
Smart Color: Blauw	Persoon
Smart Color: Geel	Persoon

2.3.1 Handmatig in-/ uitschrijven van een persoon

Wanneer je een persoon handmatig wilt in- of uitschrijven (een opt-in of opt-out wilt geven) dan gaat dit via een optie in de klantkaart.

Ga daarvoor naar de betreffende persoon. Klik door naar het tabblad 'Voorkeuren' in de klantkaart van de persoon en gebruik de knop <Persoon in/uitschrijven> om de gewenste actie uit te voeren.

Tag	Bron
Genre: Zang	Persoon
Genre: Cabaret	Persoon
Smart Color: Blauw	Persoon
Smart Color: Geel	Persoon

Wanneer je op deze knop klikt, verschijnt een scherm om een opt-in of opt-out vast te leggen. Om dit correct en AVG-compliant te verwerken, is meer informatie nodig dan alleen een vinkje. Vul daarom alle velden zorgvuldig in:

- **Kanaal:** Geef aan via welk kanaal de opt-in of opt-out is doorgegeven, bijvoorbeeld 'Telefonisch' wanneer een opt-out is vastgelegd na een klacht via de telefoon.
- **Omschrijving:** Noteer kort de reden of wijze van wijziging, zodat deze later eenvoudig te herleiden is.
- **Type:** Selecteer het juiste type opt-in, zodat de persoon de juiste berichten wel of niet ontvangt.
- **Opt-in:** Geef aan of het gaat om een aanmelding (vinkje) of een afmelding (geen vinkje).
- **Datum:** De datum en tijd worden automatisch ingevuld op het moment dat je de actie uitvoert.

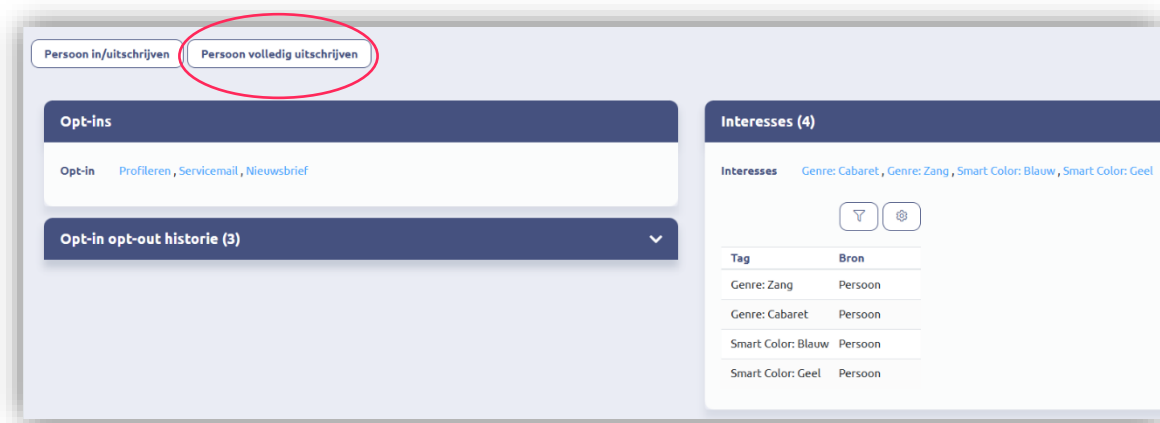
The screenshot shows a web interface for managing a person's subscription status. At the top, there is a red header with a back arrow and the text '< Persoon: Tobias (T.) van Est'. Below this is the main title 'Persoon in/uitschrijven' in red. A grey box indicates '1 Persoon geselecteerd: Tobias (T.) van Est'. The instruction 'Geef de in te voegen waarden op.' is followed by several fields: 'Kanaal' with a dropdown menu showing 'Handmatig', 'Omschrijving' with a text area containing 'Handmatige inschrijving voor de nieuwsbrief', 'Type' with a dropdown menu showing 'Nieuwsbrief', 'Opt-in' with a checked checkbox, and 'Datum' with the value '22-06-2023 09:53'. An 'OK' button is located at the bottom right.

2.3.2 Persoon volledig uitschrijven

Wanneer een persoon aangeeft om volledig uitgeschreven te willen biedt het SMP een eenvoudige optie.

Ga daarvoor naar de betreffende persoon. Klik door naar het tabblad 'Voorkeuren' in de klantkaart van de persoon en gebruik de knop '<Persoon in/uitschrijven>' om de gewenste actie uit te voeren.

Met deze functie wordt een persoon voor alle beschikbare opt-ins direct uitgeschreven, inclusief de profileren opt-in, waardoor er ook geen klantberekeningen meer worden gemaakt voor deze persoon.



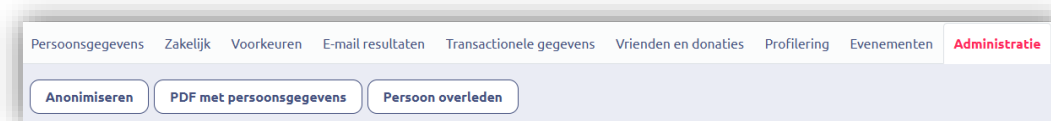
2.4 Anonimiseren

Anonimiseren is het onomkeerbaar verwijderen of aanpassen van persoonsgegevens, zodat deze niet langer herleidbaar zijn tot een individu. Binnen de AVG is dit een belangrijk middel om privacy risico's te beperken. Zodra gegevens volledig geanonimiseerd zijn, vallen ze niet langer onder de reikwijdte van de AVG.

Dit biedt organisaties de mogelijkheid om data te blijven gebruiken voor bijvoorbeeld analyses of rapportages, zonder dat dit inbreuk maakt op de privacy van betrokkenen.

Anonimiseren is daarmee essentieel voor het verantwoord verwerken van gegevens, zeker in situaties waarin het bewaren van persoonsgegevens niet langer noodzakelijk of gerechtvaardigd is. Het draagt bij aan dataminimalisatie, één van de kernprincipes van de AVG, en verkleint de impact van mogelijke datalekken.

In het SMP heb je als gebruiker de mogelijkheid om een persoon te anonimiseren. Om te anonimiseren ga je in de klantkaart naar het tabblad 'Administratie' en klik je op de knop <Anonimiseren>.

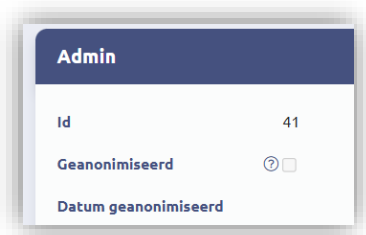


Bij het anonimiseren worden de volgende gegevens geanonimiseerd:

1. Persoonsgegevens zoals volledige naam, volledig adres, e-mailadres en telefoonnummer(s)
2. Gevoelige persoonsgegevens zoals IBAN nummer, BSN nummer etc. (indien opgeslagen in het SMP)
3. Gevoelige gegevens zoals schenkingsaktes, overeenkomsten etc. (indien opgeslagen in het SMP)

Wanneer een persoon is geanonimiseerd, dan wordt dit aangegeven d.m.v. een vinkje in de klantkaart bij het veld 'Geanonimiseerd' en de datum van uitvoering bij 'Datum

geanonimiseerd. Deze velden zijn te vinden binnen de klantkaart op het 'Administratie' tabblad, binnen de sectie 'Admin'.



Nadat een persoon eenmaal geanonimiseerd is verdwijnt de knop <Anonimiseren> in het tabblad 'Administratie'.

2.5 Bewaartermijnen en doorlopend anonimiseren

Als organisatie ben je zelf verantwoordelijk voor het tijdig anonimiseren van persoonsgegevens. Met het bovenstaande proces kun je handmatig een persoon anonimiseren wanneer dat nodig is.

De AVG schrijft voor dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld. Het hanteren van duidelijke bewaartermijnen is daarom essentieel. Zodra de bewaartermijn is verstreken en de gegevens niet langer nodig zijn, moeten deze worden verwijderd of geanonimiseerd. Dit helpt voorkomen dat verouderde of onnodige gegevens onbedoeld worden gebruikt of in verkeerde handen terechtkomen.

Door heldere bewaartermijnen te combineren met tijdige anonimisering, voldoe je als organisatie aan belangrijke beginselen van de AVG, zoals dataminimalisatie en doelbinding.

Wanneer er binnen je organisatie duidelijke richtlijnen gelden voor bewaartermijnen en de voorwaarden voor anonimisering, dan is het verstandig dit proces te automatiseren. Zo weet je zeker dat het altijd tijdig en correct gebeurt, zonder dat hier handmatige acties voor nodig zijn.

Doorlopend anonimiseren is een proces dat op maat wordt ingericht en afgestemd op de behoeften van jouw organisatie. Denk hierbij aan:

- Inzichtelijk maken welke databronnen binnen jouw organisatie aanwezig zijn
- Vaststellen van de juiste bewaartermijnen per bron
- Het technisch inrichten van het geautomatiseerd anonimiseren binnen het SMP

Wil je hierover advies en dit laten inrichten? Neem dan gerust contact op met jouw primaire contactpersoon bij Smart Connections of via het Support contactformulier.

2.6 Bouncers

Een bouncer is een persoon in de database van wie het e-mailadres om welke reden dan ook niet bereikbaar is, waardoor verzonden e-mails niet afgeleverd kunnen worden en terugkaatsen.

Er zijn grofweg twee soorten bounces:

1. Hard bounce: het e-mailadres bestaat niet (meer), is verkeerd gespeld of is permanent onbereikbaar
2. Soft bounce: het e-mailadres is tijdelijk onbereikbaar, bijvoorbeeld door een volle inbox of een technische storing bij de ontvangende mailserver

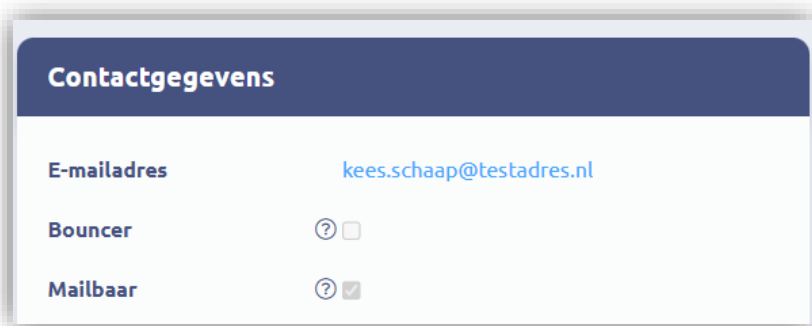
Wanneer binnen het SMP drie pogingen op rij resulteren in een bounce, dan wordt een persoon gemarkeerd als bouncer. Er wordt een vinkje gezet in het veld '**Bouncer**'. Dit veld is terug te vinden in de klantkaart binnen het tabblad Persoonsgegevens in de 'sectie' Contactgegevens'.

Dit veld kan handmatig worden uitgevinkt om een nieuwe verzendpoging te doen, bijvoorbeeld:

- Wanneer het e-mailadres is gewijzigd
- Of wanneer het adres slechts tijdelijk onbereikbaar was (bijvoorbeeld door een volle mailbox)

Door het vinkje te verwijderen, wordt het e-mailadres weer vrijgegeven voor verzendingen. Het veld 'Valide e-mailadres' wordt herzien naar '1. Valide'.

Zodra het e-mailadres van een persoon is gemarkeerd als bouncer dan wordt het veld 'Mailbaar' uitgevinkt. De persoon wordt daarmee uitgesloten in alle selecties waar dit als conditie is opgenomen.



The screenshot shows a form titled 'Contactgegevens' with a dark blue header. Below the header, there are three rows of data:

Contactgegevens	
E-mailadres	kees.schaap@testadres.nl
Bouncer	☐
Mailbaar	☒

Waarom is dit belangrijk?

Het structureel bijhouden van bouncers draagt bij aan:

- Een schoner en betrouwbaarder adressenbestand
- Betere resultaten van je e-mailcampagnes
- Het voorkomen van reputatieschade bij e-mailproviders

2.7 PDF met persoonsgegevens

Het is onder de AVG verplicht om, indien gewenst, relaties inzicht te geven in alle persoonsgegevens welke je van hen hebt opgeslagen.

In het SMP is het mogelijk om met één simpele druk op de knop alle relevante persoonsgegevens te exporteren, inclusief die uit het transactionele model.

Je maakt hiervoor gebruik van de knop <PDF met persoonsgegevens>. Je vindt deze op het 'Administratie' tabblad binnen de klantkaart. Wanneer je op deze knop drukt wordt er een PDF document gegenereerd met alle in het platform beschikbare gegevens van de betreffende persoon.



2.8 Zoekvraag maken voor een nieuwsbrief

Bij het opstellen van een zoekvraag (selectie) om een campagne te verzenden, zijn twee zoekcriteria verplicht:

- **Opt-in:** Selecteer binnen de dropdown het gewenste opt-in type. Op deze manier worden alleen personen met de juiste opt-in voor deze campagne geselecteerd.
- **Mailbaar:** Stel binnen het zoekveld 'Mailbaar' de waarde in op 'Ja'. Dit veld geeft aan dat de persoon mailbaar is, oftewel: niet overleden, geen bouncer en in het bezit van een geldig e-mailadres.

Filter Kolommen Sortering Meer ...

☐ Uitgebreid

Id		Zoek tot en met
Voornaam		
Achternaam		
E-mailadres		
Postcode		
Opt-in	Nieuwsbrief	
Interesses		
Mailbaar	Ja	
Groep		
Relatietype		

+ Voeg een zoekveld toe

Na het instellen van deze verplichte criteria kun je de selectie naar wens verder verfijnen met aanvullende zoekvoorwaarden.

3 Waar moet je zelf op letten?

Het zorgvuldig omgaan met persoonsgegevens gaat verder dan alleen het gebruik van het SMP. Ook in je dagelijkse werkzaamheden kom je in aanraking met persoonsgegevens of heb je hier toegang toe. Het is daarom belangrijk om altijd alert te blijven op hoe je hiermee omgaat.

Hieronder vind je enkele praktische tips:

- Verwerk alleen persoonsgegevens als dat noodzakelijk is voor je werk. Vraag je altijd af: heb ik deze gegevens echt nodig? Minder gegevens betekent minder risico.
- Werk bij voorkeur in beveiligde systemen. Sla persoonsgegevens niet onnodig lokaal op (zoals op je bureaublad, in Excel of Word documenten).
- Vergrendel altijd je scherm als je je werkplek verlaat:
 - Windows: Windows-toets + L
 - Mac: Control + Command + Q
- Gebruik voor elk systeem een uniek en sterk wachtwoord. Handige tools voor het veilig beheren van wachtwoorden zijn bijvoorbeeld Roboform, KeePass of Dashlane.
- Hergebruik nooit wachtwoorden
- Bewaar wachtwoorden nooit in je browser
- Stuur geen bestanden met persoonsgegevens via e-mail of WeTransfer. Gebruik hiervoor een beveiligde SFTP-server. Wanneer dit echt onvermijdelijk is, verstuur dan een ingepakt bestand (bijvoorbeeld via WinZip) met een apart gedeeld wachtwoord.
- Wil je een bestand door Smart Connections laten verwerken, bijvoorbeeld voor een import? Lever dit dan veilig aan via:
<https://smartconnections.crmplatform.nl/uploaden>

4 Begrippenlijst

Begrip	Toelichting
Anonimiseren	Dit is een bijzondere verwerking van persoonsgegevens. Bij anonimiseren verwijder je alle gegevens die herleidbaar zijn tot een unieke persoon. Zodra gegevens zijn geanonimiseerd, zijn het geen persoonsgegevens meer en is de AVG niet langer van toepassing.
AVG	Voluit: Algemene Verordening Gegevensbescherming. De Europese privacywet die geldt voor alle bedrijven binnen de EU. De AVG is de Nederlandse vertaling van de GDPR.
Beveiligingsincident en datalek	Het is belangrijk een onderscheid te maken tussen een beveiligingsincident en een datalek. De wet noemt een beveiligingsincident formeel een "inbreuk op de beveiliging". Dit is een gebeurtenis die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van, of ongeoorloofde toegang tot persoonsgegevens die zijn verzonden, opgeslagen of anderszins verwerkt. Voorbeelden van beveiligingsincidenten: • Kwijtgeraakte of gesloten USB-stick of laptop • Hack • Geslaagde ransomware-aanval • Versturen van persoonsgegevens naar een verkeerde ontvanger • Converteren van persoonsgegevens via een online tool • Onbedoeld verstrekken van wachtwoorden aan onbevoegden • Onbeheerd achterlaten van een onbeveiligde computer in een publieke ruimte • Versturen van een brief met gevoelige gegevens naar de verkeerde persoon Een datalek is een beveiligingsincident dat daadwerkelijk een risico vormt voor de rechten en vrijheden van betrokken personen, bijvoorbeeld het risico op identiteitsfraude.
Bewaartermijn	Persoonsgegevens mogen niet langer bewaard worden dan nodig is voor het doel waarvoor ze zijn verzameld. Er moet een wettelijke grondslag zijn om gegevens langer te bewaren. Enkele voorwaarden:

	• Bewaartermijnen moeten worden opgenomen in het verwerkingsregister. Advies: bewaar data maximaal vijf jaar na het einde van de actieve relatie met een persoon. • Betrokkenen moeten geïnformeerd worden over de bewaartermijn via het privacy statement. • Bewaar- en vernietigingstermijnen moeten, waar mogelijk, vertaald worden naar passende technische en organisatorische maatregelen. • Na het verstrijken van de bewaartermijn moeten persoonsgegevens definitief verwijderd of geanonimiseerd worden.
GDPR (zie AVG)	General Data Protection Regulation, de Engelstalige naam voor de AVG. De termen GDPR en AVG zijn synoniem.
Meldplicht datalek	Overheden en bedrijven moeten een (ernstig) datalek direct melden bij de Autoriteit Persoonsgegevens. In zulke gevallen moet ook de betrokkene worden geïnformeerd.
Opt-in nieuwsbrief	Toestemming om nieuwsbrieven te ontvangen, meestal van commerciële aard. Binnen dit type opt-in kunnen subgroepen of benamingen worden gebruikt, zoals Educatie, Jongeren, Zakelijk, etc
Opt-in profileren	Toestemming voor verwerking en analyse van persoonsgegevens met als doel het voorspellen van gedrag. Deze opt-in wordt automatisch geactiveerd na aanmelding. Afmelden kan alleen per brief of telefoon. Profileren moet altijd vermeld worden in het privacy statement, inclusief hoe men zich kan afmelden. Het privacy statement moet op elk formulier waar persoonsgegevens worden gevraagd of getoond beschikbaar zijn.
Opt-in servicemail	Toestemming om klanten te voorzien van algemene, niet-commerciële servicegerelateerde informatie. Deze opt-in staat standaard aan bij personen waarmee het bedrijf een relatie heeft.
Persoonsgegevens	Alle informatie die direct of indirect kan herleiden tot een natuurlijk persoon.
Privacyverklaring of privacy statement	Document waarin wordt beschreven welke persoonsgegevens worden verzameld, hoe deze worden verwerkt en voor welke doeleinden.
Profileren	Elke geautomatiseerde verwerking van persoonsgegevens waarbij bepaalde persoonlijke aspecten van een persoon worden geëvalueerd, met als doel zijn situatie, voorkeuren, gedrag, locatie of verplaatsingen te analyseren of voorspellen.

Recht op inzage en Recht om vergeten te worden	Betrokkenen hebben het recht om inzicht te krijgen in hun gegevens en om verzoeken tot verwijdering daarvan in te dienen.
Toestemming (van een klant)	In het privacy statement moet worden vermeld dat personen bezwaar kunnen maken tegen het bewaren van hun persoonsgegevens en hoe zij dat kunnen doen. Je kunt deze persoon dan handmatig anonimiseren.
Verantwoordelijke	De natuurlijke persoon of organisatie die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt.
Verwerken van persoonsgegevens	Alle handelingen met persoonsgegevens, zoals ontvangen, opslaan, lezen, bewerken, doorsturen, anonimiseren, mailen, analyseren, verwijderen, etc.
Verwerker	De partij die persoonsgegevens verwerkt namens de verantwoordelijke.
Verwerkersovereenkomst	Een overeenkomst tussen verantwoordelijke en verwerker waarin wordt vastgelegd: • Welke persoonsgegevens worden verwerkt en met welk doel • De rechtmatigheid van de verwerking • Waar de gegevens zijn opgeslagen • Hoe de beveiliging is geregeld • Of de verwerker samenwerkt met subverwerkers
Verwerkingsregister	Het register met alle verwerkingsactiviteiten van persoonsgegevens binnen een organisatie. De AVG schrijft voor welke informatie hierin moet worden opgenomen. Zie voor meer informatie: <u>Autoriteit Persoonsgegevens - Verantwoordingsplicht</u>

