meldregister

meldregister is een product van Maray Digital · meldregister.nl · support@meldregister.nl

Verwerkersovereenkomst

Versie 1.3, 8 november 2026

Deze verwerkersovereenkomst hoort bij de algemene voorwaarden van meldregister en geldt voor elke organisatie die meldregister gebruikt.

Partijen

1. De organisatie die een abonnement op meldregister afsluit via meldregister.nl of een voorstel van Maray Digital aanvaardt, hierna **de Organisatie**. De Organisatie is verwerkingsverantwoordelijke.
2. **Maray Digital**, gevestigd aan de Oostdorpseweg 18, 3176 PL Poortugaal, ingeschreven bij de Kamer van Koophandel onder nummer 42139108, hierna **Maray Digital**. Maray Digital is verwerker.

Overwegingen

De Organisatie gebruikt meldregister om incidenten, overlast en (bijna-)ongevallen op haar vestigingen te laten melden en op te volgen. Daarbij verwerkt Maray Digital persoonsgegevens in opdracht van de Organisatie. De Algemene verordening gegevensbescherming (AVG) vraagt dat partijen daarover schriftelijke afspraken maken. Dat doen zij in deze overeenkomst, die de afspraken uit artikel 28 van de AVG bevat.

1. Begrippen

De begrippen persoonsgegevens, verwerken, verwerkingsverantwoordelijke, verwerker, betrokkene, inbreuk in verband met persoonsgegevens (datalek) en toezichthoudende autoriteit hebben de betekenis die de AVG eraan geeft. **De Overeenkomst** is het abonnement of het voorstel op grond waarvan de Organisatie meldregister gebruikt, inclusief de algemene voorwaarden. **De Dienst** is meldregister: het meldformulier, het portaal, de meldingen per mail, push en sms, en de bijbehorende opslag.

2. Onderwerp en duur

1. Maray Digital verwerkt persoonsgegevens uitsluitend om de Dienst aan de Organisatie te leveren, zoals beschreven in Bijlage 1.
2. Deze overeenkomst geldt zolang de Overeenkomst loopt en daarna zolang Maray Digital nog persoonsgegevens van de Organisatie onder zich heeft.

3. Bij strijd tussen deze overeenkomst en de algemene voorwaarden gaat voor de verwerking van persoonsgegevens deze overeenkomst voor.

3. Instructies

1. Maray Digital verwerkt de persoonsgegevens alleen op basis van schriftelijke instructies van de Organisatie. De Overeenkomst, deze overeenkomst en de instellingen die de Organisatie zelf in het portaal kiest (zoals rollen, vestigingen, escalatieregels en bewaartermijnen) gelden als die instructies.
2. Maray Digital verwerkt de persoonsgegevens niet voor eigen doeleinden, verkoopt ze niet en gebruikt ze niet om de Organisatie, haar medewerkers of betrokkenen te profileren.
3. Vindt Maray Digital dat een instructie in strijd is met de AVG of andere wetgeving, dan laat zij dat de Organisatie direct weten.
4. Verplicht het recht van de Europese Unie of van een lidstaat Maray Digital tot een verwerking, dan meldt zij dat vooraf aan de Organisatie, tenzij de wet dat verbiedt.

4. Verplichtingen van de Organisatie

1. De Organisatie bepaalt het doel en de grondslag van de verwerking en zorgt dat die rechtmatig zijn. Dat geldt in het bijzonder voor gegevens van strafrechtelijke aard (zoals een aangifte of de inschakeling van de politie) en voor gegevens over kinderen.
2. De Organisatie informeert haar medewerkers, ouders, verzorgers en andere betrokkenen over het gebruik van meldregister, bijvoorbeeld in haar privacyverklaring, op de meldposter of in het personeelshandboek.
3. De Organisatie beheert zelf wie toegang heeft tot het portaal, welke rol iemand heeft en welke vestigingen iemand ziet, en haalt toegang weg zodra die niet meer nodig is.
4. De Organisatie voert alleen persoonsgegevens in die voor het melden en opvolgen nodig zijn. Voor kinderen gebruikt zij het interne casusnummer en geen naam; meldregister vraagt daar ook niet om.

5. Geheimhouding

1. Maray Digital houdt de persoonsgegevens geheim en legt dezelfde verplichting op aan iedereen die onder haar gezag werkt.
2. Technisch beheer van Maray Digital bekijkt gegevens in de database of op de server alleen om een storing te verhelpen of op verzoek van de Organisatie. Het platformbeheer van Maray Digital heeft in het portaal geen toegang tot de dossiers van de Organisatie.

6. Beveiliging

1. Maray Digital neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen verlies en tegen onrechtmatige verwerking. De maatregelen staan in Bijlage 2.

2. Maray Digital houdt de maatregelen bij de stand van de techniek en mag ze verbeteren. Zij verlaagt het beschermingsniveau niet zonder de Organisatie daarover vooraf te informeren.
3. De Organisatie is zelf verantwoordelijk voor de beveiliging aan haar kant: zorgvuldig gebruik van accounts en herstelcodes, het geheimhouden van de vestigingscode en het beheer van de apparaten waarop meldingen binnenkomen.

7. Subverwerkers

1. De Organisatie geeft Maray Digital toestemming om de subverwerkers uit Bijlage 3 in te schakelen. Maray Digital legt die subverwerkers verplichtingen op die ten minste gelijkwaardig zijn aan die uit deze overeenkomst en blijft tegenover de Organisatie verantwoordelijk voor hun werk.
2. Wil Maray Digital een subverwerker toevoegen of vervangen, dan laat zij dat ten minste dertig dagen van tevoren weten per e-mail aan de beheerders van de Organisatie en op de pagina Veiligheid en privacy van meldregister.nl.
3. De Organisatie kan binnen die dertig dagen schriftelijk en gemotiveerd bezwaar maken. Partijen zoeken dan samen naar een oplossing. Lukt dat niet, dan mag de Organisatie de Overeenkomst opzeggen tegen de datum waarop de wijziging ingaat; vooruitbetaalde bedragen voor de periode daarna betaalt Maray Digital terug.
4. Betalingen voor het abonnement lopen via Mollie. Mollie verwerkt betaalgegevens als zelfstandige verwerkingsverantwoordelijke en is geen subverwerker onder deze overeenkomst.

8. Verwerking buiten de Europese Economische Ruimte

1. Maray Digital bewaart de persoonsgegevens binnen de Europese Unie en verwerkt ze daar.
2. Pushmeldingen gaan via de pushdienst van het apparaat van de ontvanger (Google, Apple of Mozilla). Die berichten zijn onderweg versleuteld en bevatten alleen het meldnummer, de soort, de ernst en de vestiging, nooit namen of de omschrijving van een melding. De Organisatie kan push uitzetten en alleen mail en sms gebruiken.
3. Pushberichten naar de Meldregister-app voor iPhone en Android lopen via Apple en Google, die daarvoor als subverwerker in Bijlage 3 staan. Zo'n bericht is onderweg versleuteld en zegt alleen dat er een nieuwe melding is en hoe ernstig die is, zonder namen, vestiging of omschrijving. Wie in de app push uitzet, krijgt geen pushberichten meer.
4. Voor andere verwerkingen buiten de Europese Economische Ruimte is de voorafgaande schriftelijke instemming van de Organisatie nodig, en gelden de waarborgen die de AVG daarvoor vraagt.

9. Bijstand

1. Maray Digital helpt de Organisatie om verzoeken van betrokkenen (inzage, verbetering, verwijdering, beperking, bezwaar, overdraagbaarheid) te beantwoorden. De Organisatie kan de meeste verzoeken zelf afhandelen in het portaal: dossiers zoeken, aanpassen, exporteren en verwijderen. Lukt dat niet,

dan helpt Maray Digital binnen tien werkdagen na een verzoek.

2. Ontvangt Maray Digital zelf een verzoek van een betrokkene over gegevens van de Organisatie, dan stuurt zij dat verzoek door naar de Organisatie en handelt zij het niet zelf af.
3. Maray Digital helpt de Organisatie, voor zover redelijk, bij een gegevensbeschermingseffectbeoordeling en bij voorafgaande raadpleging van de toezichthouder. De technische bijlage bij de DPIA stelt Maray Digital op verzoek beschikbaar.
4. Bijstand die meer dan incidenteel werk vraagt, mag Maray Digital tegen haar gebruikelijke uurtarief in rekening brengen; zij laat dat vooraf weten.

10. Datalekken

1. Ontdekt Maray Digital een inbreuk in verband met persoonsgegevens die de Organisatie raakt, dan meldt zij dat zonder onredelijke vertraging en uiterlijk binnen 48 uur na ontdekking aan de beheerders van de Organisatie, zodat de Organisatie binnen de wettelijke termijn van 72 uur de toezichthouder kan informeren.
2. De melding bevat wat op dat moment bekend is: de aard van de inbreuk, de categorieën en het geschatte aantal betrokkenen en gegevens, de waarschijnlijke gevolgen en de genomen of voorgestelde maatregelen. Wat later bekend wordt, volgt zo snel mogelijk.
3. Maray Digital werkt mee aan het onderzoek, beperkt de gevolgen en helpt bij de melding aan de toezichthouder en aan betrokkenen. Melden aan de toezichthouder en aan betrokkenen doet de Organisatie zelf, tenzij partijen anders afspreken.

11. Controle

1. Maray Digital geeft de Organisatie op verzoek de informatie die nodig is om te beoordelen of deze overeenkomst wordt nageleefd.
2. De Organisatie mag ten hoogste één keer per jaar, met een aankondiging van dertig dagen, een controle laten uitvoeren door haarzelf of door een onafhankelijke deskundige die tot geheimhouding verplicht is. De controle vindt plaats onder werktijd, verstoort de Dienst niet en beperkt zich tot de verwerkingen onder deze overeenkomst. De Organisatie draagt de kosten van de controle; Maray Digital draagt de kosten van haar eigen medewerking, tenzij de controle ernstige tekortkomingen aantoont.
3. Is er een concrete aanwijzing van een inbreuk of een eis van de toezichthouder, dan geldt de beperking tot één keer per jaar niet.

12. Bewaren, teruggave en verwijderen

1. De Organisatie stelt in het portaal de bewaartermijn per ernstniveau in. Na afloop van de termijn anonimiseert meldregister een afgeronde melding automatisch: naam, omschrijving, notities, betrokkenen en bijlagen worden verwijderd, de statistiek (soort, ernst, vestiging, datum) blijft.

2. Zolang de Overeenkomst loopt, kan de Organisatie haar gegevens zelf exporteren in het portaal (CSV). Bijlagen levert Maray Digital op verzoek aan.
3. Eindigt de Overeenkomst, dan blijft het portaal tot de einddatum beschikbaar om te exporteren. Daarna verwijdert Maray Digital alle persoonsgegevens van de Organisatie binnen dertig dagen, tenzij een wettelijke plicht langer bewaren vereist. Kopieën in back-ups verdwijnen daarna door de normale rotatie van de back-ups, binnen vijfendertig dagen.
4. Op verzoek bevestigt Maray Digital schriftelijk dat de verwijdering is uitgevoerd.

13. Aansprakelijkheid

1. Iedere partij is aansprakelijk voor de schade die zij door een toerekenbare tekortkoming onder deze overeenkomst of onder de AVG veroorzaakt. Een boete van de toezichthouder draagt de partij aan wie de overtreding is toe te rekenen.
2. De aansprakelijkheid van Maray Digital is per gebeurtenis of reeks samenhangende gebeurtenissen beperkt tot het bedrag dat de Organisatie in de twaalf maanden vóór de gebeurtenis voor de Dienst heeft betaald. Deze beperking geldt niet bij opzet of bewuste roekeloosheid van Maray Digital.

14. Overige bepalingen

1. Deze overeenkomst komt tot stand doordat de Organisatie bij het aanmelden op meldregister.nl akkoord gaat met de voorwaarden en de verwerkersovereenkomst, of doordat zij het voorstel van Maray Digital aanvaardt. Een ondertekend exemplaar is op verzoek beschikbaar.
2. Wijzigingen in deze overeenkomst gelden alleen als beide partijen er schriftelijk mee instemmen. Verandert de wet of een uitspraak van de toezichthouder de eisen, dan passen partijen de overeenkomst in overleg aan. Nieuwe versies van de bijlagen die het beschermingsniveau verhogen, mag Maray Digital eenzijdig doorvoeren; zij maakt ze bekend op de pagina Veiligheid en privacy.
3. Op deze overeenkomst is Nederlands recht van toepassing. Geschillen leggen partijen voor aan de rechtbank Rotterdam, nadat zij hebben geprobeerd er samen uit te komen.
4. Contact over deze overeenkomst, datalekken en verzoeken van betrokkenen: support@meldregister.nl.

Bijlage 1: beschrijving van de verwerking

Onderwerp en aard. Het leveren van meldregister: een webformulier achter een QR-code waarmee medewerkers zonder account incidenten, overlast en (bijna-)ongevallen melden, een beveiligd portaal waarin leidinggevenden meldingen opvolgen, en berichten per mail, push en sms bij een nieuwe melding of een termijn. De verwerkingen zijn: opslaan, tonen aan gebruikers volgens rol en vestiging, versturen van berichten, exporteren, samenvatten, back-uppen, anonimiseren en verwijderen.

Doel. Het registreren en opvolgen van incidenten (agressie, bedreiging, geweld, onveilige situaties), van overlast en signalen uit de omgeving van een vestiging en van (bijna-)ongevallen met kinderen en derden, ook als bewijs van het veiligheids- en gezondheidsbeleid, om medewerkers, kinderen en bezoekers te

beschermen en aan de verplichtingen uit de Arbowet en de Wet kinderopvang te voldoen.

Categorieën betrokkenen. Medewerkers van de Organisatie (melders, gebruikers van het portaal en medewerkers die bij een incident of ongeval betrokken zijn), ouders, verzorgers en andere derden die bij een incident of ongeval betrokken zijn, en kinderen (uitsluitend via een intern casusnummer, en bij een ongeval de leeftijdsgroep en de groep).

Categorieën persoonsgegevens.

GEGEVEN	VAN WIE	OPSLAG
Naam en, als de melder dat invult, e-mailadres van de melder	medewerker	versleuteld
Omschrijving van wat er gebeurde, uitkomst en notities	vrije tekst	versleuteld
Naam of omschrijving van een betrokkene en diens rol	ouder, verzorger, derde	versleuteld
Intern casusnummer van een kind	kind	versleuteld
Soort, ernst, vestiging, datum, status, termijnen		gewoon
Externe meldingen (gemeente, politie) met kenmerk en terugkoppeling		toelichting versleuteld
Locatieverbod: persoon, vestigingen, periode	ouder of derde	persoon versleuteld
Ongeval: plek, letsel en lichaamsdeel (vaste keuzes), zorg, leeftijdsgroep, ouders ingelicht	kind of derde	gewoon, zonder naam
Ongeval: groep van het kind, beschrijving van het letsel, eerste hulp, reden ouders nog niet ingelicht, idee om het te voorkomen	kind of derde	versleuteld
Foto's en documenten bij een melding		versleuteld, buiten de webroot
Gebruikers van het portaal: naam, e-mailadres, functie, mobiel nummer, rol	leidinggevenden	mobiel nummer versleuteld
Logboek: wie een dossier opende of wijzigde, wanneer	gebruikers	gewoon, zonder inhoud

Bijzondere en gevoelige gegevens. Gegevens van strafrechtelijke aard (aangifte, inschakeling van de politie), gegevens over kinderen en, bij een ongeval, gezondheidsgegevens: het soort letsel en de zorg die nodig was, als vaste keuze en zonder diagnose, gekoppeld aan een intern casusnummer en niet aan een naam. Ongevallen van medewerkers worden niet in meldregister vastgelegd. Meldregister vraagt geen burgerservicenummer; de Organisatie voert dat ook niet in. Mails, pushberichten en sms'jes bevatten nooit namen of de omschrijving van een melding, alleen het meldnummer, de soort, de ernst en de vestiging.

Bewaartermijnen. Instelbaar per ernstniveau in het portaal. Standaard 24 maanden na afronding voor ernst laag en middel, en 60 maanden na afronding voor ernst hoog en acuut. Daarna anonimiseert meldregister de melding automatisch. Logboekregels blijven zolang het dossier bestaat.

Demo-omgevingen met verzonnen voorbeeldgegevens vallen buiten deze overeenkomst.

Bijlage 2: beveiligingsmaatregelen

1. **Versleuteling op veldniveau.** Namen, omschrijvingen, notities, e-mailadressen, telefoonnummers en de vestigingscode staan versleuteld in de database (AES-256 met integriteitscontrole). Bijlagen worden versleuteld voordat ze op de schijf komen, onder een willekeurige bestandsnaam, buiten de webroot. De sleutel staat gescheiden van de back-ups en in de wachtwoordkluis van Maray Digital.
2. **Versleuteld transport.** Alle verbindingen lopen over HTTPS met HSTS. De database staat op de applicatieserver en accepteert alleen lokale verbindingen.
3. **Toegang op rol en vestiging.** Vestigingsmanagers zien alleen hun eigen vestigingen, regiomanagers de toegewezen vestigingen, directie alleen meldingen met ernst hoog en acuut en exports zonder namen. De naam van een melder die vertrouwelijk meldt, blijft voor de directie verborgen. Organisaties zijn strikt van elkaar gescheiden; dit is met geautomatiseerde tests vastgelegd.
4. **Tweestapsverificatie** is verplicht voor iedereen met een account (authenticator-app met herstelcodes). Nieuwe gebruikers krijgen een uitnodiging met beperkte geldigheid en kiezen zelf een wachtwoord van minimaal tien tekens.
5. **Melden zonder account, met twee sloten.** De link in de QR-code bevat een onraadbare sleutel per vestiging; daarnaast is een vestigingscode nodig die niet op de poster staat. Na herhaalde foute codes volgt een tijdelijke blokkade en een waarschuwing aan de beheerder.
6. **Logboek.** Elke inzage van een dossier, elke statuswijziging, elke export en elke import wordt vastgelegd met gebruiker en tijdstip.
7. **Bewaartermijnen en anonimiseren** zoals beschreven in Bijlage 1, uitgevoerd door een dagelijkse taak.
8. **Geen gegevens op het apparaat.** Het portaal bewaart geen dossiers in de browser. Op het apparaat van een melder blijven alleen de vestigingscode (dertig dagen) en een nog niet verzonden concept (ten hoogste 24 uur) staan.
9. **Beveiligingsheaders.** Pagina's van het portaal kunnen niet in een frame van een andere site worden geladen en worden niet gecachet.
10. **Hosting en back-ups.** De Dienst draait op een server van Maray Digital bij Strato in Duitsland. Die server wordt ook voor andere websites van Maray Digital gebruikt; de hostingomgeving scheidt die per abonnement en systeemgebruiker. Elke nacht wordt een back-up gemaakt op de server en als versleutelde kopie bij Scaleway in Amsterdam, alleen bereikbaar met een sleutel die uitsluitend vanaf de server werkt. Back-ups worden ongeveer vijf weken bewaard.

11. **Organisatie.** Alleen technisch beheer van Maray Digital heeft toegang tot de server, met een persoonlijke sleutel en tweestapsverificatie waar de omgeving dat ondersteunt. Updates van het platform en de onderliggende software worden regelmatig doorgevoerd. Wijzigingen worden getest voordat ze live gaan.

Bijlage 3: subverwerkers

SUBVERWERKER	DOEL	LOCATIE VAN DE VERWERKING
Strato AG	Hosting van de applicatie, de database, de bijlagen en de uitgaande e-mail	Duitsland
Scaleway SAS	Versleutelde externe kopie van de back-ups	Amsterdam, Nederland
Spryng B.V.	Versturen van sms-berichten (alleen meldnummer, soort, ernst en vestiging), als de Organisatie sms gebruikt	Nederland
Apple Inc.	Pushberichten naar de Meldregister-app op iPhone (Apple Push Notification service), alleen dat er een nieuwe melding is en de ernst	Verenigde Staten
Google LLC	Pushberichten naar de Meldregister-app op Android (Firebase Cloud Messaging), alleen dat er een nieuwe melding is en de ernst	Verenigde Staten, doorgifte op basis van het EU-VS-gegevensprivacykader

Pushmeldingen in de browser lopen via de pushdienst van het apparaat van de ontvanger (Google, Apple of Mozilla), versleuteld en zonder namen; zie artikel 8. De actuele lijst staat op meldregister.nl onder Veiligheid en privacy.