



Privacybeleid

1. Inleiding

Uw privacy is belangrijk voor ons!

Samen met de partners die deelnemen aan het CoroPrevention-consortium, streven we ernaar om volledig te voldoen aan de Algemene Verordening Gegevensbescherming (General Data Protection Regulation, GDPR) van de EU.

Deze mobiele CoroPrevention-app is alleen toegankelijk voor en te gebruiken door deelnemers aan het gepersonaliseerde preventieprogramma CoroPreventon. De mobiele app stelt u in staat om deel te nemen aan het programma en ondersteunt de gezamenlijke besluitvorming door u te herinneren aan de afgesproken doelen en medicatie-inname. Hiervoor is een regelmatige rapportage van persoonlijke gedrags-, medicatie- en parameterinformatie aan uw studieverpleegkundige nodig. Dit gebeurt door het invullen van de informatie in de app en tijdens studiebezoeken.

Als fabrikant van de CoroPrevention Tool Suite-app geven wij bij UniWeb BV de hoogste prioriteit aan het waarborgen van de beveiliging en vertrouwelijkheid van al onze diensten, systemen en de gegevens die ze bevatten. Daarom hebben we een krachtig en doeltreffend beheersysteem voor informatiebeveiliging ontwikkeld, waarvoor we het ISO 27001:2013-certificaat hebben ontvangen.

Dankzij onze strenge normen voor informatiebeveiliging kunnen we de kritieke en gevoelige informatie in onze informatiesystemen beschermen tegen misbruik of ongeoorloofd gebruik. Bovendien helpen ze ons bij het beschermen van uw persoonlijke gegevens tegen fouten, ongelukken of kwaadwillige handelingen die zouden leiden tot ongeoorloofde publicatie, openbaarmaking, wijziging, verlies of vernietiging van de gegevens.

Een uitgebreidere privacyverklaring voor het CoroPrevention-programma is te vinden op de CoroPrevention-website. In geval van tegenstrijdigheden tussen dit beleid en de CoroPrevention-privacyverklaring zal de CoroPrevention-privacyverklaring voorrang hebben op dit privacybeleid voor de mobiele CoroPrevention-app.

2. Wie heeft toegang?

Het gepersonaliseerde preventieprogramma CoroPrevention wordt uitgevoerd door de partners van het CoroPrevention-consortium.

Alleen het personeel van de onderzoekslocatie heeft toegang tot de werkelijke identiteit van de deelnemers aan het onderzoek. Gegevens die tijdens het onderzoek worden verzameld, worden gepseudonimiseerd (met een Subject ID) en versleuteld opgeslagen, zodat alleen bevoegde personen die deel uitmaken van het CoroPrevention-consortium, toegang hebben. Alle gegevens die de proefpersoon kunnen identificeren naast het Subject ID (bv. het ondertekende document van de geïnformeerde toestemming), moeten strikt vertrouwelijk door



de onderzoeker worden bewaard, behalve voor zover nodig om proefgerelateerde monitoring, controles en regelgevende inspecties mogelijk te maken.

De volledige lijst van gezamenlijke verwerkingsverantwoordelijken is te vinden in de CoroPrevention-privacyverklaring, gepubliceerd op de CoroPrevention-website.

Derden

UniWeb verkoopt of deelt nooit persoonlijke gegevens aan andere derden dan de hierboven genoemde partijen, die betrokken zijn bij het CoroPrevention-programma.

Om bepaalde diensten te kunnen leveren, doet UniWeb een beroep op externe leveranciers (bv. gecentraliseerde logging-oplossing, datacenter-hosting). Zoals voorzien in de standaardbedrijfsprocedures van UniWeb, worden alle leveranciers grondig doorgelicht alvorens gebruik te maken van hun diensten. Naleving van de AVG maakt natuurlijk deel uit van de vereisten voor alle leveranciers. UniWeb evalueert regelmatig de samenwerking met haar leveranciers en de voorwaarden van die samenwerking. De samenwerking wordt stopgezet wanneer een leverancier niet langer voldoet aan de vereisten die zijn gedefinieerd in het beheersysteem voor informatiebeveiliging van UniWeb.

Voor zover toegestaan door de toepasselijke wetgeving, kunnen uw persoonlijke gegevens worden doorgegeven aan de volgende partijen:

- Overheidsinstanties
- Auditors

3. Wat verwerken we en waarom?

UniWeb bouwt, onderhoudt en host webtoepassingen en websites in overeenstemming met de specificaties die zijn verstrekt door de verwerkingsverantwoordelijke en de partners van het CoroPrevention-consortium. De persoonlijke gegevens die door deze toepassingen en websites worden verwerkt, variëren naargelang van de verschillende gebruikersrollen en gerelateerde doeleinden die door de verwerkingsverantwoordelijke zijn gedefinieerd.

De CoroPrevention-toepassingen en het EDC-systeem verzamelen informatie, zoals (niet-limitatieve lijst):

- Patiëntidentificator (pseudoniem)
- Informatie over gezondheid, medicijnen en lichaamsbeweging
- Informatie over voeding en roken
- Gebruiksstatistieken in de applicatie, inclusief log- en verbindingsinformatie (bv. browser, IP-adres).

Het doel van deze verwerkingsactiviteiten kan zijn (niet-limitatieve lijst):

- Gezondheidsvoordelen en klinische onderzoeksdoelstellingen in overeenstemming met het onderzoeksprotocol
- Authenticatie, patiëntveiligheid en cyberbeveiliging
- Om de gebruiker herinneringen en alarmen te laten instellen



- Om de werking van de applicaties te optimaliseren.
- Om afspraken met consortiumpartners na te komen met betrekking tot de consortiumovereenkomst en wettelijke vereisten.

Op het niveau van het consortium is een gegevensbeschermingseffectbeoordeling uitgevoerd om de risico's te beoordelen en risicobeperkende maatregelen te implementeren.

Als u de inventaris wilt raadplegen of meer informatie wilt over het doel van de gegevensverwerking, neem dan contact op met uw plaatselijke studieverpleegkundige.

4. Waar bewaren we uw persoonlijke gegevens?

UniWeb heeft de volledige controle en eigenaarschap over de hardware die wordt gebruikt om uw persoonlijke gegevens te bewaren. Onze productie-, staging- en back-upservers bevinden zich in België in het beveiligde datacenter van onze hostingleverancier die gecertificeerd is volgens ISO 27001:2013 en ISO 22301:2012. Persoonlijke gegevens blijven op deze servers staan, maar kunnen op bepaalde momenten door de opdrachtgever worden geëxporteerd, uitsluitend voor onderzoeks-, veiligheids- en gebruiksanalysedoeleinden. Loginformatie wordt tijdelijk opgeslagen bij de gecentraliseerde logprovider in een datacentrum binnen de EU.

5. Hoe lang bewaren we uw persoonlijke gegevens?

Standaardbewaartermijn

Tijdens het ontwerpproces van alle websites en webapplicaties die door UniWeb worden ontwikkeld, wordt een standaardbewaartermijn en verwijderingsprocedure overeengekomen met de gezamenlijke verwerkingsverantwoordelijken volgens de wettelijke vereisten, zoals beschreven in de CoroPrevention-privacyverklaring.

Voor klanten van UniWeb geldt dat alle persoonlijke gegevens die in overeenstemming met de overeenkomst via onze productieservers zijn verwerkt, kort na afloop van de overeenkomst uit onze systemen worden verwijderd. De gegevens worden binnen 180 dagen (of zoals gespecificeerd in de overeenkomst) ook volledig verwijderd uit onze back-ups.

Als onderdeel van onze operationele standaardprocedures die worden beschreven in ons beheersysteem voor informatiebeveiliging, evalueert UniWeb regelmatig de noodzaak om informatie te bewaren, zodat wij gegevens niet langer bewaren dan absoluut noodzakelijk is.

Uitzonderingen

Afwijkingen van de standaardbewaartermijn kunnen nodig zijn:

- als wettelijke verplichting



- op uitdrukkelijk verzoek van de verwerkingsverantwoordelijke (waarvoor de verwerkingsverantwoordelijke de volledige verantwoordelijkheid heeft aanvaard)

Voor meer informatie over deze uitzonderingen kunt u contact opnemen met uw plaatselijke studieverpleegkundige of de CoroPrevention-privacyverklaring raadplegen die is gepubliceerd op de CoroPrevention-website.

6. Hoe zorgen we voor beveiliging?

Als bedrijf dat zich toelegt op het bouwen van veilige en krachtige mobiele en webapplicaties, verbetert en werkt UniWeb voortdurend de beveiligingsmaatregelen bij die worden geïmplementeerd om persoonlijke gegevens en andere informatie te helpen beschermen tegen ongeoorloofde toegang, wijziging, verlies of vernietiging. De volgende voorbeelden zijn slechts enkele van de beveiligingsmaatregelen die UniWeb toepast:

- Alle door UniWeb bewaarde gegevens worden zowel in rust als tijdens het transport tussen onze dienst en uw browser of toepassing versleuteld.
- Van alle gegevens wordt een volledige back-up gemaakt.
- Onze diensten worden onderworpen aan penetratietests en beschermd door Nessus-scans.
- Gecentraliseerde logoplossing voor het bewaken van de prestaties van applicaties en cyberbeveiliging.
- Onze diensten ondersteunen geavanceerde authenticatie, waaronder het gebruik van G-Suite, Office 365-accountauthenticatie en multifactorauthenticatie.

Bij een voorval op het gebied van informatiebeveiliging zal UniWeb hier onmiddellijk en adequaat op reageren in overeenstemming met de operationele standaardprocedures die zijn beschreven in het beheersysteem voor informatiebeveiliging. Net als onze beveiligingsmaatregelen worden deze procedures regelmatig herzien en bijgewerkt om te voldoen aan de steeds veranderende uitdagingen op het gebied van informatiebeveiliging.

Alle werknemers van UniWeb worden regelmatig opgeleid met betrekking tot de beste praktijken op het gebied van beveiliging en bedrijfsprocedures. Hetzelfde niveau van betrokkenheid wordt verwacht van onze leveranciers, wier diensten regelmatig worden beoordeeld (zie: [Derden](#)).

7. Wat zijn uw rechten als betrokkene?

Tijdens de procedure voor geïnformeerde toestemming zijn uw rechten als betrokkene uitgelegd en vermeld in het document voor geïnformeerde toestemming.

Deze rechten omvatten, maar zijn niet beperkt tot:

- het opvragen van informatie over uw persoonlijke gegevens.
- het aanvragen van een kopie van al uw gegevens in een standaardformaat.



U kunt uw rechten eenvoudig uitoefenen door het formulier voor geïnformeerde toestemming te raadplegen of door contact op te nemen met uw studieverpleegkundige.

8. Hoe kunt u toestemming geven?

Door zijn/haar persoonlijke gegevens te verstrekken via de mobiele applicatie of webapplicatie en zoals uitgelegd in de procedure voor geïnformeerde toestemming, geeft de betrokkene uitdrukkelijk toestemming aan de gezamenlijke verwerkingsverantwoordelijken om de gegevens te verwerken voor de aangegeven doeleinden.

Indien de verwerkingsverantwoordelijke de persoonlijke gegevens invoert in de mobiele applicatie of webapplicatie, wordt de verwerkingsverantwoordelijke verantwoordelijk geacht voor het correct informeren van de betrokkene en het verkrijgen van zijn/haar toestemming tijdens de procedure voor geïnformeerde toestemming. Zo niet, zal dit worden beschouwd als een non-conformiteit en zal UniWeb de gepaste acties moeten ondernemen zoals bepaald in de operationele standaardprocedures in het beheersysteem voor informatiebeveiliging. Alle kosten die door UniWeb worden gemaakt om deze corrigerende maatregelen te nemen, zullen ten laste worden gelegd van de verwerkingsverantwoordelijke.

Als UniWeb of een van de partners van het CoroPrevention-consortium specifieke persoonlijke gegevens aan derden wilt doorgeven, zal de gebruiker om aanvullende toestemming worden gevraagd. Het voorgaande is ook van toepassing op de verwerking van uw persoonlijke gegevens buiten de EU.

9. Met wie kunt u contact opnemen?

Als u vragen hebt over dit privacybeleid of als u een van de bovenstaande rechten als betrokkene wilt uitoefenen, neem dan contact op met uw plaatselijke studieverpleegkundige.