Privacybeleid

Innocom Bureau voor Bedrijfscommunicatie b.v.

Als ook handelsnamen, zoals CSI Service

Innocom/ CSI Service

Biesven 2

5595 DD LEENDE

Auteur:	Saskia van der Hoeven
Datum:	5 juni 2020
Versie:	3
Status:	Definitief

Inhoudsopgave

1 Documentbeheer 3
2 Kader 4
2.1 Voor wie? 4
2.2 Begrippen 4
2.3 Gerelateerde documenten 4
2.4 Doel 5
2.5 Visie 5
2.6 Kernpunten 6
2.7 Scope 8
2.8 Raakvlakken en overlap met andere beleidsthema's 10
3 Privacymanagement 12
3.1 Managementstructuur 12
3.2 Proceseigenaarschap 12
3.3 Toezicht 12
4 Privacybeleid 13
4.1 Algemeen 13
4.2 Het verwerken van persoonsgegevens 14
4.3 Kapstokregeling 14
4.4 Inachtneming bijzondere wettelijke voorschriften 14
5 Privacyservices 16
5.1 Rechten 16
5.2 Contact 17
6 Auditbeleid 18

1 Documentbeheer

Documentgegevens	
Naam	Innocom Bureau voor Bedrijfscommunicatie B.V. als ook handelsnamen, zoals CSI Service
Titel document	Privacybeleid
Onderwerp document	Privacybeleid
Versie	3
Status	Definitief
Documentnummer	20191024-01
Documentclassificatie	
Categorie	Beleidsdocument
Auteur	Saskia van der Hoeven
Documenteigenaar	
Datum eerste concept	18-06-2018, 30 juli 2018
Datum van goedkeuring	4-6-2020
Goedgekeurd door	Directie
Publicatiedatum	5 juni 2020
Bestandnaam	Privacybeleid_v0.3.docx
Trefwoorden	AVG, GDPR

Versiegeschiedenis Versienummer	Datum van goedkeuring	Wijzigingen/Redenen

Distributielijst Versienummer	Naam	Methode

2 Kader

2.1 Voor wie?

De doelgroep voor dit privacybeleid is eenieder die op enige wijze is betrokken bij Innocom, bureau voor Bedrijfscommunicatie b.v. of handelsnamen, zoals CSI Service. Dit zijn tenminste de Innocom en CSI Service medewerkers(sters), Innocom en CSI Service leden, klanten, gelieerde partners en strategische partners en de Innocom en CSI Service toeleveranciers.

2.2 Begrippen

In dit beleidsdocument worden de volgende begrippen gehanteerd:

- Persoonsgegevens: gegevens die kunnen leiden tot de identiteit van een persoon, bijvoorbeeld een naam, e-mailadres, een foto, een rol binnen een organisatie, etc.
- Betrokkene: diegene op wie de persoonsgegevens betrekking hebben, bijvoorbeeld uzelf, uw medewerkers, uw klanten, etc.
- Verwerkingsverantwoordelijke: diegene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Bijvoorbeeld binnen uw eigen organisatie bent u dat zelf.
- Verwerker: die partij aan wie de verwerkingsverantwoordelijke de verwerking heeft uitbesteed, bijvoorbeeld een payrollbedrijf, een accountant, een logistieke dienstverlener, een ict bedrijf, etc.
- Verwerking van persoonsgegevens: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
- Dienst: een installatiedienst, onderhoudsdienst, (verhuur- of service-)abonnement of een apparaat uit ons productportfolio.

2.3 Gerelateerde documenten

Dit beleid is onlosmakelijk verbonden met de volgende AVG-plichtige documenten:

- Het Informatiebeveiligingsbeleid
- Het verwerkingsregister
- Een privacyverklaring voor websitebezoekers en voor personeel en relevante derde partijen
- Een incidentenregister
- Een procedure voor de melding van een datalek
- Een richtlijn informatiebeveiliging voor personeel
- Verwerkersovereenkomsten met relevante derde partijen

2.4 Doel

Het doel van dit document is om duidelijk te maken hoe Innocom en CSI Service de AVG-compliance heeft geregeld. De Afkorting AVG staat voor: "Algemene Verordening gegevensbescherming". In Europa is deze wet bekend onder de naam GDPR wat staat voor: "General Data Protection Regulation". Ons privacybeleid en informatiebeveiligingsbeleid hebben tot doel om invulling te geven aan deze AVG bij de verwerking van persoonsgegevens. Dit geldt niet alleen voor verwerkingen van persoonsgegevens binnen ons kantoor, maar ook voor verwerkingen door of bij derden in opdracht van ons kantoor. Denk bijvoorbeeld aan het uitbesteden van verwerkingen en het opslaan van persoonsgegevens in cloud oplossingen.

2.5 Visie

Onze missie (waar staan we voor)
Als iets (flink) mis gaat, moet je (snel) kunnen communiceren.

Onze visie (waar gaan we voor)
Wij bieden de toegang tot hulp voor iedereen in een onverwachte noodsituatie. Hiervoor bieden wij, op een persoonlijke manier, eenvoudig te bedienen technologie met aansluiting op een altijd bemande alarmcentrale. Wij bewaken doorlopend de goede werking van onze oplossingen.

CSI Service is sinds 2003 een belangrijke leverancier van personenalarmering en daar zijn wij trost op. Dat doen we in heel Nederland en inmiddels daarbuiten met passie. Wij zijn specialist op het gebied van personenalarmering, toegangssystemen en zorg op afstand. Het vergroten van de veiligheid van cliënten is voor ons het ultieme doel.

In het kader van de privacywetgeving AVG die is gewijzigd per mei 2016 (en waarop sancties worden toegepast vanaf mei 2018) is het voor Innocom/ CSI Service noodzakelijk geweest om ingrijpende maatregelen te treffen om aan de strengere privacywetgeving te voldoen. Immers, in het brede dientstenpallet van Innocom/ CSI Service worden persoonsgegevens verwerkt van medewerkers, leden, klanten en derde partijen waarmee Innocom/ CSI Service intensief samenwerkt. Om deze reden besteedt Innocom/ CSI Service verwerkingen alleen uit aan een (sub)verwerker die afdoende garanties biedt betreffende het toepassen van "passende technische en organisatorische maatregelen", zodat deze verwerkingen voldoen aan de eisen en verplichtingen van de AVG en dus de rechten van de betrokkenen aantoonbaar zijn gewaarborgd.

2.6 Kernpunten

We doen er alles aan om de privégegevens ook echt privé te houden. We vragen gegevens, zodat we onze klanten zo goed mogelijk kunnen helpen. Welke gegevens we vragen en waarvoor we ze gebruiken leest u hieronder. Ook ziet u wat uw rechten zijn, wie toegang heeft tot de data en hoe lang we uw gegevens bewaren.

Benoeming van benodigde vereisten, afspraken en voorzieningen in de organisatie voor privacymanagement.

De AVG wetgeving beschrijft een aantal vereisten die binnen Innocom/ CSI Service zijn geimplementeerd. Dit zijn de volgende onderwerpen:

1. Accountability
2. Documentatieplicht
3. Functionaris gegevensbescherming optioneel
4. Privacy Impact assessment
5. Privacy by design, privacy by default
6. Dataportabiliteit
7. Transparantie-toestemming
8. Verplichtingen verwerker

Ad 1: dit is beschreven in paragraaf 3 van dit privacybeleid

Ad 2: als resultante van een AVG Compliance scan, uitgevoerd in september 2017 door Rsult-IT Security B.V. zijn de benodigde documenten geproduceerd:

- Privacybeleid
- Informatiebeveiligingsbeleid
- Verwerkingsregister
- Incidentenregister
- Meldplicht Datalekprocedure
- Privacyverklaring Website en medewerkers
- Verwerkersovereenkomsten met derde partijen

Ad 3: INNOCOM verwerkt niet op grote schaal bijzondere persoonsgegevens en dus is een FG niet verplicht. Wel hebben wij een Functionaris Gegevensbeschermer en die is bereikbaar via FG@csiservice.nl

Ad 4: Gezien de aard van de werkzaamheden van de organisatie (zie paragraaf 4) is het niet noodzakelijk een DPIA uit te voeren

Ad 5: Privacy by design wordt actief toegepast vanaf september 2017 in de contacten met leden, derde partijen en productleveranciers. Privacy by default is mede afhankelijk van de mogelijkheden die de gebruikte applicaties bieden op het gebied van dataverwijdering.

Ad 6: Medewerkers, Leden, cliënten en samenwerkende partijen van Innocom/ CSI Service kunnen volledig inzage krijgen in hun persoonsgegevens (voor zover die verwerkt worden) en een digitale kopie hiervan kan beschikbaar gesteld worden.

Ad 7: In alle contracten, overeenkomsten en publicaties wordt uitvoerig aandacht besteed waarom en welke persoonsgegevens worden verwerkt.

Ad 8: Daar waar Innocom/ CSI Service als verwerker optreedt is voldaan aan alle wettelijke verplichtingen, onder andere:

- Documentatieplicht, zie Ad 2 hierboven
- Innocom/ CSI Service handelt uitsluitend in opdracht van een verantwoordelijke
- Er is een FG aangesteld
- Innocom/ CSI Service heeft een datalekprocedure ingericht om de verantwoordelijke te informeren
- Er worden geen sub-verwerkers ingeschakeld zonder medeweten van de verantwoordelijke
- Innocom/ CSI Service verleent volledige medewerking en inzage aan een verzoek van de toezichthouder, indien gevraagd
- Innocom/ CSI Service heeft alle verplichte en noodzakelijke technische en organisatorische maatregelen geimplementeerd die van toepassing zijn conform de AVG richtlijnen en de ISO 27000 normeringen voor informatiebeveiliging

Persoonsgegevens kunnen op een aantal manieren verzameld worden wanneer u gebruikt maakt van de diensten van Innocom/ CSI Service. In de bijlage volgt een overzicht van de informatie die Innocom/ CSI service kunnen verzamelen. Er wordt per verschillende dienst aangegeven welke persoonsgegevens verwerkt worden of kunnen worden. Tevens wordt een onderscheid gemaakt tussen de gegevens die wij verwerken van klanten en gegevens van zorgprofessionals die gebruik maken van de dienst. Het overzicht geeft weer welke persoonsgegevens verwerkt worden, voor welk doel, op welke wettelijke grondslag de verwerking berust en hoe lang de persoonsgegevens opgeslagen worden.

Indien u uw persoonsgegevens niet aan Innocom en/of CSI Service verschaft of op enige andere wijze bezwaar maakt tegen het gebruik van uw persoonsgegevens door Innocom en/of CSI Service, kan dat ervoor zorgen dat u belemmerd wordt in het gebruik van de dienst. Hieronder wordt per verwerkingsgrondslag aangegeven wat de gevolgen zijn van het niet verschaffen van of bezwaar maken tegen verwerking van persoonsgegevens. Welke persoonsgegevens onder welke verwerkingsgrondslag vallen, kunt u per dienst terugvinden in de bijlage.

<u>Verwerkingen op grond van een wettelijke verplichting van Innocom/ CSI Service:</u>

- Wij kunnen uw toegang tot de dienst blokkeren of beperken en wij behouden ons het recht voor om de overeenkomst te beëindigen overeenkomstig onze algemene voorwaarden. De persoonsgegevens die in dit onderdeel worden vermeld, zijn vereist om te voldoen aan onze wettelijke verplichtingen.

<u>Verwerkingen noodzakelijk voor de uitvoering van de overeenkomst:</u>

- U kan worden belemmerd in het gebruik van de dienst, het is mogelijk dat de dienst niet goed functioneert. Wij kunnen uw toegang tot de dienst blokkeren of beperken en wij behouden ons het recht voor om de overeenkomst te beëindigen overeenkomstig onze algemene voorwaarden. De persoonsgegevens die in dit onderdeel worden vermeld, zijn vereist om de dienst goed te laten functioneren of te kunnen verrichten.

  Verwerkingen noodzakelijk voor de gerechtvaardigde belangen van Innocom/ CSI Service:

- Wij kunnen uw toegang tot de dienst blokkeren of beperken en wij behouden ons het recht voor om de overeenkomst te beëindigen overeenkomstig onze algemene voorwaarden. De persoonsgegevens die in dit onderdeel worden vermeld, zijn vereist om te voldoen aan de gerechtvaardigde belangen van Innocom/ CSI Service en om misbruik van de dienst en beveiligingsincidenten te voorkomen.

  Verwerkingen waarvoor uw uitdrukkelijke toestemming vereist is:

- U wordt in beginsel niet belemmerd in het gebruik van de dienst. Het weigeren of intrekken van toestemming heeft geen negatieve gevolgen voor uw gebruik van de dienst. Dit is anders bij gebruik van de dienst telemonitoring. U kan worden belemmerd in het gebruik van de dienst telemonitoring, het is mogelijk dat de telemonitoring niet goed functioneert. De persoonsgegevens die in dit onderdeel worden vermeld, zijn vereist om de telemonitoring goed te laten functioneren of te kunnen verrichten. Aangezien het om gevoelige persoonsgegevens gaat is echter uw uitdrukkelijke toestemming vereist voor het mogen verwerken van deze persoonsgegevens.

  Verwerkingen waarvoor uw toestemming vereist is:

- U wordt niet belemmerd in het gebruik van de dienst. Het weigeren of intrekken van toestemming heeft geen negatieve gevolgen voor uw gebruik van de dienst.

2.7 Scope

Dit privacybeleid is toepasbaar op de activiteiten binnen Innocom/ CSI Service waarbij persoonsgegevens worden verwerkt. Volgens de privacywetgeving moeten we zeggen welke ‘juridische gronden’ we hebben om gegevens te gebruiken. We hebben gegevens nodig vanwege de contractuele afspraken tussen een klant en CSI Service, zoals een huurabonnement van een product, wellicht de aankoop van een product of het recht op garantie en bij vergoedingen vanuit een zorgverzekering. Dit is het geval bij:

- Aanmelding van een abonnement en verhuur
- Vergoedingsaanvraag bij de verzekeraar
- Bezorging & plaatsing
- Retour
- Reparatie
- Contact met onze klantenservice

- CSI zakelijk

Daarnaast kunnen we gegevens gebruiken bij ‘gerechtvaardigd belang’. Dat betekent dat we al onze klanten de meest optimale, persoonlijke service willen verlenen. Hierbij denken we altijd aan uw privacy. Dit geldt voor:

- Reviews & klanttevredenheidsonderzoek
- Contact met onze klantenservice
- Bezoek van de website
- Accounts in de ‘mijn CSI Service’-omgeving
- Nieuwsbrief & e-mail
- Persoonlijk advies
- Acties
- Social media
- Beveiliging, wifi & camera’s

We kunnen ook een wettelijke verplichting hebben om gegevens te gebruiken, bijvoorbeeld wanneer we op basis van onze algemene voorwaarden een dienst beeindigen. En soms heeft een klant ons zelf toestemming gegeven om gegevens te gebruiken, zoals bij een automatische incasso.

Wie heeft toegang tot privacy gevoelige gegevens?

We geven je gegevens alleen door aan andere partijen als dat echt nodig is voor onze dienstverlening. Het betreft dan deze partijen in de keten volgens het ketenkeurmerk WDTM: bezorgpartners, alarmcentrale, (professionele) zorgopvolger. In het kader van een vergoedingswens kunnen wij gegevens ook doorgeven aan de door de klant zelf opgegeven zorgverzekering.
De partijen die van ons toegang krijgen tot gegevens, mogen deze alleen gebruiken om een dienst te leveren namens CSI Service. Tenzij ze zelf verantwoordelijk zijn voor het verkrijgen en beschermen van de privacygevoelige gegevens. Sommige cookie-ontwikkelaars hebben toegang tot de gegevens die cookies op onze website verzamelen. U leest hier meer over in ons cookiestatement en het privacybeleid van deze partijen. We verkopen gegevens nooit aan derden.

Waar worden gegevens opgeslagen?

We slaan gegevens op in verschillende databases. We hanteren altijd strenge beveiligingsmaatregelen. Bijna altijd slaan wij gegevens op binnen de Europese Unie. In het uitzonderlijke geval dat klantgegevens worden doorgegeven naar landen buiten de Europese Unie, zorgen we ervoor dat privacy op een passende manier beschermd blijft. Voor een aantal landen is dit officieel vastgesteld. Sommige Amerikaanse partijen hebben zich geregistreerd onder het Privacy Shield dat voldoende bescherming biedt. Of we werken met officiële modelcontracten die speciaal zijn opgesteld om privacy te waarborgen.

Hoe lang bewaren we gegevens?

We bewaren en gebruiken jouw gegevens niet langer dan noodzakelijk. Daarna verwijderen we alle data die we hebben. Of gebruiken we gegevens anoniem, omdat we bepaalde data nodig hebben voor interne analyses en rapportages zoals trainingsdoeleinden en levensduur apparaten.
We houden bepaalde (wettelijke) termijnen aan, waarna we gegevens verwijderen. Dit geldt voor:

- Opgenomen telefoongesprekken verwijderen we standaard na 30 dagen tenzij we een wettelijke verplichting hebben om een gesprek langer te bewaren.
- Camerabeelden van ons kantoor bewaren we niet langer dan 4 weken. Tenzij we iets verdachts zien dat we verder moeten onderzoeken of de beelden langer bewaard moeten worden vanwege een andere wettelijke verplichting.
- Inactieve klantaccounts verwijderen we na 7 jaar. Na die periode gebruiken we gegevens alleen anoniem, voor interne rapportages.
- Van de Belastingdienst moeten we onze administratie met factuur-, verhuur- en abonnementsgegevens 7 jaar bewaren. Daarna gebruiken we alleen anonieme gegevens voor interne rapportages.
- Van de Zorgverzekeraar moeten we onze administratief met factuur-, verhuur- en abonnementsgegevens 7 jaar bewaren. Daarna gebruiken we alleen anonieme gegevens voor interne rapportages. Een klant moet zelf ook de facturen goed bewaren, voor wanneer bijvoorbeeld de verzekering daarom vraagt.
- Laat u een product door CSI Service repareren of vervangen, bewaren we de melding en contactgegevens 7 jaar. Daarna gebruiken we je gegevens alleen anoniem, voor interne rapportages.
- Wanneer u een mobiel abonnement voor een mobiele dienst via CSI Service hebt afgesloten bewaren we het contract met de telecomprovider verplicht 7 jaar. Na die periode gebruiken we geanonimiseerde gegevens voor interne rapportages.
- Als u zich hebt ingeschreven voor de nieuwsbrief of toestemming hebt gegeven voor het ontvangen van gepersonaliseerde berichten, dan bewaren we die toestemming 5 jaar lang. Ook als je op een gegeven moment beslist dat je de nieuwsbrief of gepersonaliseerde berichten niet meer wilt ontvangen, bewaren we het intrekken van je verzoek. Na die periode gebruiken we gegevens alleen anoniem, voor interne rapportages.
- Gegevens die we gebruiken om fraude te voorkomen bewaren we heel lang.

2.8 Raakvlakken en overlap met andere beleidsthema's

De Innocom/ CSI Service heeft in haar eigen handboek een aantal beleidsthema's beschreven. Dit betreft kwaliteit, risicomanagement, informatiebeveiliging, personeel en organisatie, en communicatie naar externe relaties.

Daar waar de AVG verplichtingen oplegt om deze beleidsuitgangspunten aan te scherpen heeft Innocom/ CSI Service aanpassingen doorgevoerd aan deze publicaties.

3 Privacymanagement

Binnen het kader van het AVG accountabilityprincipe heeft de Innocom/ CSI Service directie deze verantwoordelijkheid erkend en zij heeft een informatiebeveiligingsbeleid opgesteld, intern gecommuniceerd en zal een correcte naleving van dit beleid afdwingen.

3.1 Managementstructuur

De directeur operationele zaken van Innocom/ CSI Service, Jan Verasdonck is de eindverantwoordelijke voor privacy en security zaken aangaande de AVG. Hij wordt hierin bijgestaan door Functionaris Gegevensbescherming en een gelieerde privacy en security specialist.

3.2 Proceseigenaarschap

De directeur operationele zaken is de proceseigenaar van het privacymanagement, en hij is bevoegd om taken te delegeren, maar blijft eindverantwoordelijk. Een voorbeeld van een taak die gedelegeerd is het systeembeheer van de infrastructuur.

3.3 Toezicht

Innocom/ CSI Service zal jaarlijks een controle uitvoeren door middel van een "Privacy Control Framework" om te toetsen of aan alle AVG verplichtingen zijn voldaan. Dit onderzoek zal met een externe daartoe gekwalifiseerde partij plaatsvinden.

4 Privacybeleid

4.1 Algemeen

Uitgangspunt en taakstelling van de organisatie.

Innocom/ CSI Service verwerkt persoonsgegevens van klanten, leden, gelieerde adviseurs en eigen medewerkers. Deze betrokkenen kunnen erop vertrouwen dat Innocom/ CSI Service zorgvuldig en vertrouwelijk hun persoonsgegevens verwerkt, conform de verplichtingen van de AVG. Van alle medewerkers en gelieerde adviseurs wordt verwacht dat zij in lijn met dit beleid integer, vertrouwelijk en zorgvuldig met persoonsgegevens omgaan. De uitgangspunten waaraan Innocom/ CSI Service zich heeft gecommiteerd zijn de volgende:

- Rechtmatigheid, behoorlijkheid, transparantie
    - Persoonsgegevens worden in overeenstemming met de wet op behoorlijke en zorgvuldige wijze verwerkt
- Grondslag en doelbinding
    - Innocom/ CSI Service zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen op basis van een wettelijke grondslag verwerkt
- Dataminimalisatie
    - Innocom/ CSI Service verwerkt alleen strikt noodzakelijke persoonsgegevens voor het vooraf bepaalde doel. Wij streven naar minimale gegevensverwerking. Daar waar mogelijk worden minder of geen persoonsgegevens verwerkt
- Bewaartermijnen
    - Persoonsgegevens worden niet langer bewaard dan noodzakelijk, en er wordt rekening gehouden met de wettelijke bewaarplicht
- Beschikbaarheid, integriteit en vertrouwelijkheid
    - Persoonsgegevens zijn op de gewenste momenten alleen beschikbaar voor geautoriseerde medewerkers. Innocom/ CSI Service bewaakt de juistheid van de gegevens en zorgt ervoor dat deze niet benaderbaar zijn voor onbevoegden
- Derde partijen en data uitwisseling
    - Innocom/ CSI Service werkt samen met derde partijen waarbij sprake is van gegevensverwerking van persoonsgegevens. Met deze partijen maakt Innocom/ CSI Service afspraken waar gegevensuitwisseling aan moet voldoen conform de wettelijke verplichtingen. Deze afspraken worden periodiek getoetst
- Rechten van betrokkenen
    - Innocom/ CSI Service honoreert alle rechten van betrokkenen tenzij dit door beperkingen vanuit wet- en regelgeving niet mogelijk is
    -

4.2 Het verwerken van persoonsgegevens

Beschrijving van typen verwerkingen die binnen de organisatie noodzakelijk zijn.

INNOCOM verwerkt persoonsgegevens van medewerkers, stagiares, leden, klanten en aangesloten derde partijen conform de overeenkomsten en/of wettelijke verplichtingen met deze betrokkenen. Bij elke verwerking met genoemde betrokkenen beoordelen wij of INNOCOM verwerkingsverantwoordelijke of verwerker is en wat het doel en de grondslag is van de verwerking. Dit is per bedrijfssproces nader uitgewerkt en dit wordt voordurend bijgewerkt in ons register van verwerkingsactiviteiten. INNOCOM conformeert zich aan de daarbij behorende beginselen en verplichtingen die voortvloeien uit de wet- en regelgeving AVG.

4.3 Kapstokregeling

Innocom/ CSI Service werkt met externe adviseurs die door Innocom/ CSI Service gekoppeld worden aan klanten waarmee Innocom/ CSI Service een relatie heeft. Dit geldt ook voor prospects die Innocom/ CSI Service heeft benaderd.

Deze externen treden op als verwerkingsverantwoordelijken (en dus niet als verwerker) maar er is een gedeelde verantwoordelijkheid richting de betrokkenen. Dit betekent dat Innocom/ CSI Service met deze externe adviseurs duidelijke privacy afspraken maakt om de rechten van de betrokkenen te beschermen. Deze afspraken zijn contractueel vastgelegd.

4.4 Inachtneming bijzondere wettelijke voorschriften

Wij zullen ervoor zorgen dat we passende technische en organisatorische beveiligingsmaatregelen nemen voor de verwerking van persoonsgegevens. Wij volgen algemeen geaccepteerde standaarden ter bescherming van persoonsgegevens, zowel tijdens de overdracht daarvan en zodra we de persoonsgegevens hebben ontvangen. Wij hebben in ieder geval de volgende maatregelen genomen:

- Toegang tot onze servers en infrastructuur is alleen mogelijk vanaf bepaalde beveiligde servers vanaf specifieke IP adressen en is alleen mogelijk door middel van een specifieke combinatie van sleutels.
- Toegang tot onze database is enkel mogelijk door middel van drietrapsauthenticatie en persoonlijke accounts die beschermd zijn met een gebruikersnaam en wachtwoord. Enkel personen die toegang tot de database nodig hebben voor hun taak, krijgen een dergelijk account.
- We hanteren een wachtwoordbeleid om sterke wachtwoorden te garanderen. Wachtwoorden moeten periodiek opnieuw ingesteld worden.
- Er is een firewall aanwezig die automatisch geconfigureerd wordt door middel van beveiligingsscripts.
- We gebruiken virtual private clouds per aparte omgeving (testen, acceptatie en productie) om risico's te beperken.

- Opgeslagen gegevens zijn beveiligd middels encryptie. Wachtwoorden worden tevens gehasht. Lokaal opgeslagen gegevens (bijvoorbeeld op iOS en Android) wordt tevens versleuteld opgeslagen voor zover het gevoelige informatie betreft (medische informatie of authenticatie informatie).
- We gebruiken SSL (Secure Socket Layer)-technologie om transmissie data naar ons te versleutelen
- Het maximaal aantal foutieve login pogingen is beperkt.
- Alle informatie die gebruikers invoeren wordt gecontroleerd om er zeker van te zijn dat geen schadelijke data wordt geüpload.
- Er is software geïnstalleerd om schadelijke software tijdig op te sporen.
- Beveiligingsupdates vinden plaats op maandelijkse basis.
- We monitoren toegang tot de back-end sectie om mogelijk inbreuken op de beveiliging of andere afwijkingen te kunnen detecteren.
- We maken dagelijks een back-up van de database. Gebruikers die toegang hebben tot de database hebben geen toegang tot de back-ups om het ongewenst verwijderen van databases te voorkomen.
- Cookies bevatten geen volledige authenticatie informatie zoals wachtwoorden.
- Informatie in cookies wordt verwijderd als u uitlogt.
- Belangrijke informatie in cookies wordt versleuteld.
- De duur van inlogsessies is beperkt in de tijd.
- Er is beleid omtrent het gebruik van datadragers (zoals laptops en USB-sticks).
- Toegang tot het pand is beperkt en het pand is beveiligd.

U moet er rekening mee houden dat onze Verwerkers verantwoordelijk zijn voor het verwerken, beheren of opslaan van (een deel van) de persoonsgegevens die we ontvangen. Verwerkers zijn niet bevoegd om deze gegevens te gebruiken om bij u te adverteren. Deze Verwerkers zijn contractueel, door middel van een verwerkersovereenkomst, met ons verplicht om de persoonsgegevens die zij van ons hebben ontvangen, te beveiligen.

Er is echter geen manier van overbrengen via het internet of een methode van elektronische opslag die 100% veilig is. Daarom kunnen we de absolute veiligheid niet garanderen.

5 Privacyservices

5.1 Rechten

Beschrijving van rechten van betrokkenen/burgers

De betrokkenen hebben het recht om hun gegevens in te zien, te wijzigen, vergeten te worden (mits rekening wordt gehouden met de wettelijke bewaartermijnen), gegevens over te dragen en de betrokkenen heeft het recht op informatie.

Houd er rekening mee dat het verwijderen van persoonsgegevens kan leiden tot de beëindiging van het recht om gebruik te maken van de dienst.

Wij behouden ons het recht voor om uw persoonsgegevens in onze bestanden te behouden indien wij van mening zijn dat dit noodzakelijk of aan te bevelen is om de dienst aan anderen te verstrekken, geschillen op te lossen, de toepasselijke gebruiksvoorwaarden te handhaven, voor technische en/of juridische vereisten en/of indien de dienst dat vergt.

Om per e-mail toegang te krijgen tot de eigen persoonsgegevens, moet u voldoende bewijs van uw identiteit verstrekken zoals wij dat verzoeken. We behouden ons het recht voor om elke gebruiker toegang te weigeren als we van mening zijn dat er vragen zijn over uw identiteit. Wij reageren binnen 4 weken op alle toegangsverzoeken. Bij complexe verzoeken kan de termijn met nog eens 4 weken worden verlengd. Indien wij de termijn verlengen, zullen wij u binnen 4 weken na het indienen van het verzoek daarvan op de hoogte stellen.

U kunt ons verzoeken om de verwerking van uw persoonsgegevens in de toekomst te beperken of te stoppen. Wij voldoen aan uw verzoek, maar u kunt worden belemmerd in uw gebruik van de dienst en het kan mogelijk zijn dat u de dienst niet meer kan of mag gebruiken.

U kunt ons met redelijke tussenpozen verzoeken om de persoonlijke informatie die wij over u verwerken, zoals door u gespecificeerd, over te dragen, zolang de gevraagde informatie geen persoonlijke gegevens bevat van andere natuurlijke personen en zolang als de gevraagde informatie is verwerkt met als grondslag uw toestemming of dat verwerking noodzakelijk is voor het uitvoeren van de dienst. Wij zullen uw verzoek binnen 4 weken na ontvangst van het verzoek voldoen.

U heeft het recht om bij de bevoegde privacy autoriteit een klacht in te dienen die verband houdt met onze verwerking van persoonsgegevens. Voor Nederland is deze autoriteit de Autoriteit Persoonsgegevens, die u kunt bereiken op https://autoriteitpersoonsgegevens.nl/

5.2 Contact

Handelwijze en beantwoordingsproces bij vragen intern of extern

Voor vragen en / of opmerkingen aangaande de privacywetgeving kan de betrokkene terecht bij de Functionaris Gegevensbescherming van Innocom/ CSI Service via email: FG@csiservice.nl

6 Auditbeleid

Innocom/ CSI Service zelf zal jaarlijks een audit uitvoeren en de resultaten hiervan met een in privacy gespecialiseerde partij evalueren.

De entiteiten die geaudit zullen worden zijn de organisatie, de techniek, de medewerkers, de derde partijen en er zal een check plaatsvinden op de juridische contracten.