Informatiebeveiligings- en privacybeleid

Stamtafel

2019 – 2021

Stamtafel - iZorgd! B.V.

Vastgesteld op 01-05-2020

0. Aanleiding/inleiding

Stamtafel faciliteert op een laagdrempelige, sociale en veilige manier het samenspel tussen zorgverlener en de persoon die gebaat is bij zelfregie over de eigen zorg. Dit doet Stamtafel door de formele en informele zorg samen aan een (digitale) tafel te zetten in de overzichtelijke Stamtafel app. Hierdoor worden communicatie barrières weggenomen en gaat de kwaliteit van leven omhoog.

Stamtafel wil dit samenspel tussen zorgverlener zo makkelijk mogelijk maken op een manier waarbij de mens centraal staat én diens privacy. Privacy is daarbij niet alleen iets om rekening mee te houden, maar is een doel op zich.

Privacy is een ruim begrip. In dit document verstaan we hieronder dat persoonsgegevens moeten worden beschermd en dat daar op passende wijze mee om moet worden gedaan. In het beschermen van persoonsgegevens ligt een raakvlak met informatiebeveiliging. Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Informatiebeveiliging gaat om het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Deze informatie omvat persoonsgegevens, maar ook andere informatie.

Aandacht voor zowel informatiebeveiliging als privacy is vereist om ervoor te zorgen dat de vertrouwelijkheid van persoonsgegevens van gebruikers van de Stamtafel geborgd blijft. Door middel van dit beleid wordt een duidelijke richting gegeven aan informatiebeveiliging en privacy en laat Stamtafel zien dat zij de privacy van haar gebruikers waarborgt, beschermt en handhaaft.

1. Doel en scope van het beleid

Stamtafel wil partijen veilig met elkaar in verbinding brengen. Dat betekent dat gebruikers erop moeten kunnen vertrouwen dat Stamtafel zorgvuldig en veilig met hun persoonsgegevens omgaat.

Het **doel van dit beleid** is het aantoonbaar borgen van aandacht voor privacy en informatiebeveiliging en het beheersen van de risico's en incidenten op dat gebied zodat gebruikers en andere belanghebbenden er gerechtvaardigd op kunnen vertrouwen dat Stamtafel zorgvuldig omgaat met hun persoonlijke informatie. Dit doel wordt in het volgende hoofdstuk voorzien van concrete uitgangspunten.

De **scope** van dit beleid is als volgt. Het informatiebeveiligings- en privacybeleid is van toepassing op de gehele organisatie, dat wil zeggen op zowel eigen als ingehuurde medewerkers en op alle samenwerkingspartners.

2. Concrete uitgangspunten

De volgende uitgangspunten worden gehanteerd bij de realisatie van dit beleid:

- Stamtafel voldoet aan de toepasselijke wet- en regelgeving;
- Dat geldt in het bijzonder voor de Algemene Verordening Gegevensbescherming en de daarin genoemde uitgangspunten zoals dataminimalisatie, de eisen van subsidiariteit en proportionaliteit en de ontwerpprincipes 'privacy by default en by design';
- Voor zover relevante regelgeving mogelijk niet dwingend voor Stamtafel geldt, zal Stamtafel zoveel mogelijk handelen conform de daarin genoemde uitgangspunten. Hierbij kan worden gedacht aan NEN7510 (Informatiebeveiliging in de zorg) en NTA 7516 (Uitwisseling gezondheidsgegevens met een zorgprofessional);

- Stamtafel is 'in control' over haar informatie en kijkt kritisch naar waar haar data wordt opgeslagen. Dat is bij voorkeur in de EER en anders landen daarbuiten die voldoende bescherming bieden, zoals doorgifte op basis van adequaatheidsbeslissingen.
- Gebruikersinformatie blijft waar mogelijk in eigen beheer en wordt niet opgeslagen op lokale devices. Bedrijfsmiddelen worden actief beheerd;
- Verantwoordelijkheden tussen Stamtafel en derden, zoals leveranciers zijn duidelijk belegd;
- Medewerkers worden continue getraind in het herkennen van risico's op het gebied van informatiebeveiliging en privacy en weten hoe zij in dergelijke situaties moeten handelen;
- (Ingehuurd) personeel wordt zorgvuldig geselecteerd waarbij eisen met betrekking tot informatiebeveiliging en privacy in acht worden genomen. Al het personeel dient te beschikken over een relevante Verklaring Omtrent Gedrag;
- Stamtafel selecteert betrouwbare leveranciers die voldoen aan gangbare beveiligingstandaarden. Voor zover van toepassing wordt met de leveranciers vooraf een verwerkersovereenkomst gesloten;
- Gangbare beveiligingsnormen worden toegepast, zoals in ieder geval tijdige patching, encryptie en toegangsbeheer. Ook voor de ontwikkel- en testomgeving worden de nodige veiligheidsmaatregelen getroffen;
- Er wordt gekozen voor betrouwbare en veilige technieken, zoals het Laravel development framework.
- Stamtafel voert periodiek pentesten en audits uit op haar platform;
- Stamtafel past fysieke beveiliging toe om te voorkomen dat onbevoegde personen toegang hebben tot haar informatiesystemen;
- Berichten en gesprekken van gebruikers zijn vertrouwelijk. Ze kunnen alleen door de geadresseerden of deelnemers van groepsgesprekken worden ingezien, niet door andere personen.
- Stamtafel is transparant naar gebruikers in de wijze waarop met hun persoonsgegevens wordt omgegaan.

3. Categorieën persoonsgegevens

Binnen Stamtafel zijn grofweg drie categorieën van betrokkenen te onderscheiden: gebruikers, personeel en partners. Binnen deze categorieën worden verschillende categorieën van persoonsgegevens verwerkt.

a. Gebruikers

Voor het gebruik van Stamtafel dienen gebruikers een gebruikersaccount aan te maken. Daarbij worden de volgende persoonsgegevens gevraagd:

- Voornaam
- Achternaam
- E-mailadres
- Biografie (optioneel)

Bijzondere persoonsgegevens, zoals medische persoonsgegevens worden niet uitgevraagd. Gebruikers wordt in de gebruikersovereenkomst nadrukkelijk afgeraden om dit soort gegevens te delen. Voor het delen van medische gegevens wordt aangesloten bij de communicatiekanalen van de zorgprofessional. Ondanks het voorgaande, kan het per ongeluk voorkomen dat een gebruiker toch medische gegevens deelt in berichten of in het kader van groepsgesprekken, foto's of videogesprekken, maar alleen in ongestructureerde vorm. Stamtafel zal alle berichten en gesprekken daarom zo goed mogelijk beveiligingen en vertrouwelijk behandelen.

b. Personeel

Stamtafel dient als werkgever diverse persoonsgegevens van medewerkers te registreren. Het gaat om NAW-gegevens, contactgegevens, opleidingsgegevens, functie, salaris, BSN-nummers en geldigheidsduur van identiteitsdocumenten en ziekteverzuimgegevens. Bijzondere persoonsgegevens worden alleen verwerkt als hiervoor een wettelijke grondslag bestaat. Datzelfde geldt voor de gegevens van ingehuurd personeel.

c. Partners

Met andere partners, zoals leveranciers of opdrachtgevers worden ook gegevens uitgewisseld. Het gaat hierbij voornamelijk om contactgegevens zoals:

- Voornaam
- Achternaam
- (zakelijk) e-mailadres
- (zakelijk) telefoonnummer

Voor de voornoemde en volgende persoonsgegevens worden door Stamtafel de volgende bewaartermijnen gehanteerd:

Bewaartermijnen

Persoonsgegeven	Bewaartermijn	Toelichting
Ziektegegevens bedrijfsarts / re-integratie[1]	10-15 jaar	Door hulpverleners, voor werkgever geldt periode van 2 jaar.
Subsidieadministratie	10 jaar	Artikel 4:69 Awb
Financiële gegevens / boekhouding	7 jaar	Artikel 52 AWR
Loonbelastingverklaringen / kopie identiteitsdocument werknemer	5 jaar	Artikel 66 lid 4 Uitvoeringsregeling LB
Gegevens personeelsdossier (ook ziekteverzuim)	2 jaar (na uitdiensttreding)	Autoriteit Persoonsgegevens / Vrijstellingenbesluit[2]
Arbeidsongeschiktheidgegevens	2 jaar (na beëindiging dienstverband)	Wet Verbetering Poortwachter
Contactgegevens partners	2 jaar (na laatste contact)	-
Logfiles	6 maanden	Vrijstellingenbesluit
Concurrentiebedingafspraken	Zolang de termijn loopt	-
Opleidingsafspraken	Zolang de termijn loopt	Vrijstellingenbesluit
Gebruikersgegevens	Voor de duur dat het gebruikersaccount actief is, daarna worden de gegevens binnen 2 weken verwijderd	-
Loonbeslagen	Tot opheffing	-

4. Verwerkingsdoeleinden

Voor elke verwerking van persoonsgegevens moet een rechtmatige grondslag aanwezig zijn. Dat betekent dat de verwerking alleen mag plaatsvinden op één van de wettelijke gronden. Stamtafel stelt daarom altijd een doel vast voor de verwerking. Voor Stamtafel betekent dit dat persoonsgegevens alleen mogen verwerkt op basis van de volgende gronden:

[1] Zie uitgave 'De zieke werknemer – beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers', Autoriteit Persoonsgegevens, 23 februari 2016.

[2] Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp)

- Om een verplichting na te komen die in de wet staat, zoals het bijhouden van de boekhouding. Daarin zijn persoonsgegevens van werknemers opgenomen die op grond van de wet 7 jaar moeten worden bewaard.
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was. Hierbij gaat het voornamelijk om de gebruikersovereenkomst die met gebruikers wordt gesloten en op grond waarvan minimale persoonsgegevens moeten worden verwerkt.[3]
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking. Hiervan is alleen in uitzonderingssituaties sprake, bijvoorbeeld wanneer het gaat om ongestructureerde informatie geplaatst uit eigen beweging van de gebruiker.[3]
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke of een derde. Daarbij wordt de normuitleg van de Autoriteit Persoonsgegevens gevolgd.[4] Voor een concreet voorbeeld moet worden gedacht aan verwerkingen die noodzakelijk zijn om het technisch functioneren van Stamtafel mogelijk te maken of te verbeteren. [3]

De verwerkingsdoeleinden zijn per verwerking opgenomen in het verwerkingsregister.

5. Rechten van betrokkenen

Personen van wie persoonsgegevens worden verwerkt (de zogenoemde ‘betrokkenen’) hebben op grond van de AVG verschillen rechten met betrekking tot deze gegevens. Deze rechten gelden in het bijzonder voor gebruikers van Stamtafel, maar ook zoveel mogelijk voor eigen medewerkers.

Alle gebruikers (en overige betrokkenen) waarvan door Stamtafel persoonsgegevens worden verwerkt, hebben de volgende rechten:

- Recht op informatie: gebruikers mogen vragen hoe hun persoonsgegevens worden verwerkt.
- Inzagerecht: gebruikers mogen hun gegevens inzien om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt. Gebruikersgegevens zijn op ieder moment inzichtelijk voor de gebruiker.
- Correctierecht: als duidelijk wordt dat de gegevens niet kloppen, kan de gebruiker een verzoek indienen om deze te corrigeren.
- Intrekken toestemming: eventuele toestemming voor het verwerken van persoonsgegevens kan op ieder moment worden ingetrokken.
- Recht op dataportabiliteit: gebruikers hebben het recht te vragen om hun persoonsgegevens over te dragen.
- Recht om vergeten te worden: dit betekent dat de gebruiker het recht heeft om zijn of haar persoonsgegevens door Stamtafel te laten vergeten. Net zoals bij het verwijderen van de gebruikersaccount zal Stamtafel alle gegevens van de gebruiker op zijn of haar verzoek wissen.
- Recht op beperking van de verwerking; in bepaalde situaties heeft de gebruiker het recht op beperking van het gebruik van zijn of haar gegevens te vragen. Dat is bijvoorbeeld het geval als de gegevens onjuist of niet meer nodig zijn.
- Recht op bezwaar: gebruikers hebben op grond van de wet het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. Stamtafel zal dit altijd respecteren.

Stamtafel is wettelijk verplicht om binnen 4 weken op verzoeken te reageren. De privacyfunctionaris of Functionaris Gegevensbescherming zal toezien op de tijdige opvolging van dergelijke verzoeken.

[3] Zie het Stamtafel Privacy Statement versie 1.3 voor een nadere omschrijving van het doel en de grondslag.

[4] Zie het document “Normuitleg grondslag ‘gerechtvaardigd belang’”, zonder datum. Toegankelijk via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf

Betrokkenen hebben daarnaast recht op informatie over de verwerking van hun persoonsgegevens. Stamtafel heeft hiervoor een afzonderlijk Privacy Statement geformuleerd. Dit Privacy Statement wordt actueel gehouden en in ieder geval bij inschrijving met gebruikers gedeeld.

6. Privacy maatregelen

Om te privacy van betrokkenen te waarborgen heeft Stamtafel nog enkele specifieke maatregelen getroffen:

- Stamtafel heeft een ethisch manifest vastgesteld, waarin is opgenomen dat gegevens van de gebruiker altijd van de gebruiker blijven. De gebruiker bepaalt met wie hij of zij informatie deelt. Stamtafel deelt nooit gegevens met anderen.
- Stamtafel houdt een verwerkingsregister bij. Dit register wordt tenminste 1x per half jaar geactualiseerd.
- Stamtafel heeft een procedure ingesteld voor datalakken. Datalekken worden conform de leidraad van de Autoriteit Persoonsgegevens gemeld.
- Stamtafel heeft logging op haar systemen en applicaties geactiveerd. Dit om te kunnen achterhalen welke medewerkers persoonsgegevens van kandidaten of andere gevoelige informatie hebben verwerkt. Gelogde activiteiten worden alleen gericht doorzocht bij vermoedens van misstanden.
- Stamtafel voert voorafgaand aan wijzigingen/updates van het Stamtafel platform gegevensbeschermingseffectbeoordeling (of PIA's) uit als de wijziging een impact heeft op (lees: een risico kan vormen voor) de privacy van betrokkenen.

7. Verantwoordelijkheden en rollen

Dit informatiebeveiligings- en privacybeleid wordt uitgevoerd door verschillende betrokken personen en rollen binnen Stamtafel. Ten aanzien van de verantwoordelijkheden voor de uitvoering van het beleid onderkent Stamtafel de volgende rollen:

Eigenaar:
De directie is als eigenaar eindverantwoordelijk voor de uitvoering van het informatiebeveiligings- en privacybeleid en daarmee het voldoen aan wetten en normen. De eigenaar is daarnaast verantwoordelijk voor het:

- Het in control zijn over informatie;
- Het trainen van medewerkers;
- Het organiseren van periodiek overleg met onderstaande betrokkenen;
- Het borgen van de toepassing van voornoemde en andere beveiligingsmaatregelen door middel van in ieder geval een jaarlijkse directiebeoordeling.

Information Security Officer:
De ISO is verantwoordelijk voor het onderhouden van het informatiebeveiligings- en het privacybeleid (dat laatste in samenwerking met de Privacyfunctionaris/Functionaris Gegevensbescherming). De taken van de ISO bestaan verder uit:

- Het voorbereiden van een jaarlijkse directiebeoordeling, waaronder:
    - Het actualiseren van dit beleid;
    - Het beoordelen of dit beleid effectief is, door een GAP-analyse te doen naar de uitgangspunten en huidige situatie;
    - Het doen van verbetersuggesties.
- Het opstellen van een auditplan ten aanzien van het Stamtafel platform en het rapporteren van de bevindingen;
- Het laten uitvoeren van pentesten en audits;

- Het proactief adviseren op het gebied van informatiebeveiliging;

Privacyfunctionaris/Functionaris Gegevensbescherming:
De Privacyfunctionaris of FG heeft een onafhankelijke rol en is toezichthouder rondom de naleving van de wet- en regelgeving met betrekking tot privacy en gegevensbescherming. Deze functionaris ziet toe op de naleving van de privacyregelgeving binnen de organisatie, waaronder in het bijzonder de verzoeken van betrokkenen. Samen met de ISO wordt het informatiebeveiligings- en privacybeleid onderhouden.

Productowner:
De Productowner zorgt ervoor dat informatie en privacy worden ‘meegenomen’ in de ontwikkeling van het product. Alleen zo kan recht worden gedaan aan de ontwerpprincipes ‘privacy by default en by design’. Hiervoor dienen tevens tijdig de juiste personen te worden betrokken. De productowner ziet op naleving van deze principes in de test- en ontwikkelfase.

8. Herziening beleid

Dit beleid wordt jaarlijks herzien en waar nodig geactualiseerd en aangepast. Als wijzigingen in het wetgevend kader of de dienstverlening van Stamtafel daartoe aanleiding geven, wordt het beleid eerder aangepast.