Veiligheid en Voor Morgen

Dit document beschrijft alle maatregelen om de gegevens van klanten zo veilig mogelijk te verwerken. Onderstaand beschrijven we de veiligheid van diverse gebruikte systemen en processen.

Inloggen

Voor het inloggen vertrouwen wij op iDIN, het identificatiesysteem van de gezamenlijke Nederlandse banken. Het belangrijkste voordeel hiervan is dat wij met grote zekerheid kunnen zeggen dat iemand die inlogt daadwerkelijk die persoon is. Immers, iedereen die in Nederland bankiert heeft zich bij voorafgaande aan het daadwerkelijk krijgen van een eigen rekening, bij de bank moeten identificeren. Bijkomend voordeel van dit systeem is dat klanten niet nog apart een account met een wachtwoord moeten aanmaken en dat ze zouden kunnen vergeten of dat uit kan lekken.

Transport gegevens

Op alle plekken waar persoonsgegevens verplaatst worden van het ene systeem naar het andere systeem maken we gebruik van encryptie. Het meest duidelijke voorbeeld is het gebruik van het ‘slotje’ in de browser. Dit zorgt ervoor dat de communicatie tussen onze applicatie en de klant veilig en vertrouwd is.

Opslag zeer vertrouwelijke gegevens

Voor de opslag van de zeer vertrouwelijke gegevens rondom De Digitale Wilsverklaring maken wij gebruik van encryptie waar Voor-Morgen zelf ook niet de sleutel van heeft. De gegevens van een klant worden versleuteld met behulp van een code die we terugkrijgen van iDIN, en die code slaan wij zelf niet op. Mocht ooit de database uitlekken, dan zijn daardoor de belangrijkste gegevens daaruit versleuteld, zonder dat die sleutels centraal opgeslagen worden. Dit heeft ook een risico: mocht een klant zijn iDIN kwijtraken is het onmogelijk om bij de data te kunnen. Wij noch Voor-Morgen kan u die niet leveren en helpen.

Ook de video en de PDF van de Digitale Wilsverklaring worden versleuteld, die kunnen enkel met de documentcode opgehaald worden, deze code wordt gebruikt om het document te ontsleutelen.

Bovenstaande geldt niet voor klantgegevens zoals telefoonnummer, naam, bankrekeningnummer en e-mailadres. Voor-Morgen moet tot dergelijke gegevens toegang hebben om te kunnen incasseren of om u terug te betalen en of contact op te kunnen nemen met de klant. Uiteraard worden deze gegevens zoveel mogelijk conform eisen van de AVG verwerkt en met de grootst mogelijke zorg behandeld.

Backup

Alle gegevens worden zeer regelmatig/dagelijks geback-upt. Zij worden 6 maanden bewaard. Na 6 maanden worden de gegevens automatisch verwijderd/weggegooid. Alle backups worden versleuteld en op een fysiek andere plek bewaard dan de servers.

Locatie dataopslag

Alle gegevens van klanten van Voor-Morgen worden enkel opgeslagen op Nederlands grondgebied bij een Nederlandse hosting provider.