DIGITALME

de GDPR API

“60% VAN UW KLANTEN WIL HUN DATA OPVRAGEN”

Stilzitten is geen optie!

Waar krijgt u mee te maken?

Naast het bestaande recht hun persoonsgegevens bij u op te vragen, krijgen uw klanten op basis van de nieuwe Europese regels vanaf mei 2018 ook het recht om die gegevens aan een andere partij over te dragen. Diverse onderzoeken wijzen uit dat ze dat ook massaal van plan zijn1. Daar komt bij dat u voortaan een verantwoordingsplicht heeft waar het gaat om verwerking van persoonsgegevens. Dit alles leidt tot een mogelijke ketenverantwoordelijkheid waar u niet op zit te wachten.

Digital Me kan dit voor u oplossen.

Uw klanten krijgen het recht op overdraagbaarheid van hun persoonsgegevens

Het inzagerecht bestaat al heel lang, maar het is nu uitgebreid met het recht de persoonsgegevens in "een gestructureerde, gangbare en machineleesbare vorm te verkrijgen". Bovendien hebben individuen het recht gekregen "die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt".

Uw organisatie moet er op voorbereid zijn dat individuen deze nieuwe rechten daadwerkelijk (en massaal) gaan uitoefenen zodra de algemene verordening gegevensbescherming - AVG (GDPR) actief zal worden gehandhaafd (vanaf 25 mei 2018).

Als de voorspellingen ook maar voor een deel uitkomen, dan is stilzitten voor een organisatie die persoonsgegevens verwerkt geen optie. Een goede voorbereiding is belangrijk.

Verantwoordingsplicht

Onder de AVG is iedere organisatie zelf verantwoordelijk voor de naleving van de beginselen van de verwerking van persoonsgegevens.

Dit betekent dat u, in uw rol als verwerkingsverantwoordelijke, de verplichting heeft er voor te zorgen dat:

- de verwerking van persoonsgegevens rechtmatig, behoorlijk en transparant is
- u alleen die gegevens verzamelt die u ook echt nodig heeft
- de gegevens die worden verwerkt, juist zijn en zo nodig worden geactualiseerd
- u de gegevens verwijdert, zodra deze niet meer strikt noodzakelijk zijn
- u een passende databeveiliging heeft

Ketenverantwoordelijkheid

Als u persoonsgegevens die u verwerkt, doorgeeft aan een andere organisatie, blijft uw organisatie er in veel gevallen voor verantwoordelijk dat die ander de gegevens verwerkt conform de wettelijke regels. Gebeurt dat niet, dan zijn zowel uw organisatie als de andere organisatie hoofdelijk aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op de AVG.

1 De resultaten worden bevestigd door eigen onderzoek van de Qiy Foundation in Nederland.

De oplossing: de GDPR-API

Digital Me biedt een technische oplossing die is gebaseerd op het Qiy Afsprakenstelsel en waarmee individuen de mogelijkheid krijgen zelf hun rechten uit te oefenen, zonder uw organisatie daarmee 'lastig te vallen'. Door uw organisatie aan te sluiten op een duurzame en veilige infrastructuur, het Qiy Trust Framework, biedt u uw klanten toegang tot hun persoonsgegevens. Zij kunnen deze gegevens inzien, vragen om correctie of zelf opslaan of routeren naar andere partijen met behoud van de echtheidskenmerken.

Op drie manieren zorgen wij ervoor dat uw organisatie wordt ontzorgd:

1 procedureel
U krijgt geen verzoeken van (een onbekend aantal) individuen die hun rechten ten aanzien van de door uw organisatie verwerkte persoonsgegevens willen uitoefenen. U geeft hen gewoon de tools om dat zelf te doen;

2 juridisch
Door individuen zelf het beheer te geven over het al dan niet overdragen van hun persoonsgegevens doorbreekt u de keten van verantwoordelijkheid die zou ontstaan wanneer u persoonsgegevens van betrokkenen zelf zou doorleveren;

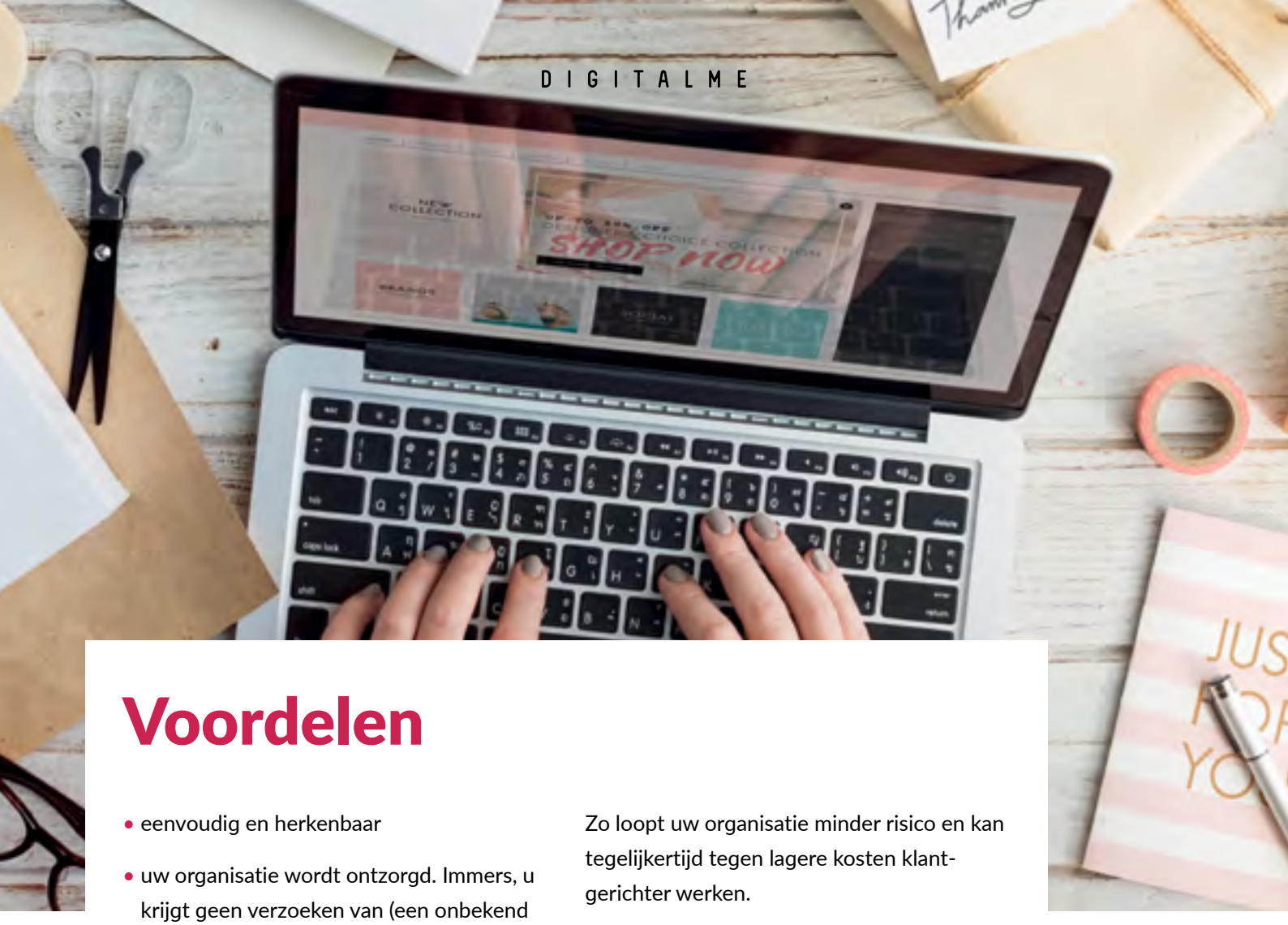
3 technisch
De voorziening waarmee individuen zelf hun persoonsgegevens kunnen inzien en/of downloaden is tegelijkertijd een voorziening die zij kunnen gebruiken voor het delen (overdragen) van hun gegevens met anderen.

de GDPR API

Hoe werkt dit dan?

Wij realiseren voor uw organisatie en voor de individuen waarvan u gegevens verwerkt, een aansluiting op het Qiy Trust Framework. Vervolgens kunnen zij hun gegevens niet alleen inzien en downloaden, maar deze ook delen met anderen (met behoud van echtheidskenmerken).

Toegang tot hun persoonsgegevens verkrijgen uw klanten door met de bestaande middelen die zij van uw organisatie hebben gekregen, in te loggen op de bestaande 'mijn'-omgeving. Vervolgens kunnen zij zelf aan de slag om hun rechten uit te oefenen. U verleent hiermee uw klanten een relevante service en u ontloopt de verantwoordelijkheid en daarmee de aansprakelijkheid die u zou hebben indien u zelf persoonsgegevens aan anderen zou doorgeven.



Voordelen

- eenvoudig en herkenbaar
- uw organisatie wordt ontzorgd. Immers, u krijgt geen verzoeken van (een onbekend aantal) individuen die hun rechten ten aanzien van hun door uw organisatie verwerkte persoonsgegevens willen uitoefenen. U geeft hen gewoon de tools om zelf hun rechten uit te oefenen
- door deze werkwijze bespaart u veel geld, omdat u geen 'human resources' behoeft vrij te maken en in te zetten voor elk binnenkomend individueel verzoek
- u voorkomt verantwoordelijkheid en daarmee aansprakelijkheid die u zou hebben indien u zelf persoonsgegevens aan anderen doorgeeft
- uw organisatie stelt het individu centraal (een uitgangspunt van de AVG)
- uw organisatie voldoet impliciet aan de uitgangspunten van de AVG van *"data protection by design and by default"*
- uw organisatie voldoet hiermee voor een groot deel aan de verplichtingen die worden voorgeschreven door de AVG

Zo loopt uw organisatie minder risico en kan tegelijkertijd tegen lagere kosten klant-gerichter werken.

Dit omdat:

- klanten veilig hun profielgegevens ter beschikking kunnen stellen: zij profileren zichzelf
- klanten (als ze dat willen) een anonieme relatie kunnen hebben met uw organisatie
- u een beveiligd '1-op-1' communicatie-kanaal met uw klanten ter beschikking heeft
- uw klanten zelf de juistheid controleren van de gegevens die u over hen heeft
- er een vertrouwensrelatie ontstaat met uw klanten die u geleidelijk kunt uitbouwen
- uw organisatie er op kan vertrouwen dat ook anonieme relaties hun verplichtingen nakomen danwel daarop kunnen worden aangesproken

GDPR – API Stappenplan

Stap 1 Alles begint met een inventarisatie van de persoonsgegevens die u verwerkt en waar deze zich bevinden. Dit kunt u zelf doen, of Digital Me doet dat voor u. Digital Me biedt u een intake gesprek inclusief voorbereiding en verslag voor € 500,- (ex BTW). Op basis daarvan kunnen er afspraken worden gemaakt over het vervolgtraject.

Stap 2 Persoonsgegevens ontsluiten op een koppelpunt dat is verbonden met uw ‘Mijn-omgeving’. Dat kan uw automatiseerder voor u regelen of een integratiespecialist.

Stap 3 Uw ‘Mijn-omgeving’ wordt door Digital Me in samenwerking met uw automatiseerder gekoppeld op het Qiy Trust Framework via de GDPR-API. Via een Qiy QR-code verkrijgen individuen een veilige en betrouwbare ‘1-op-1’ relatie met uw organisatie en hebben zij eenvoudig en veilig toegang tot hun persoonsgegevens.

Om de Qiy QR-code te scannen is een app nodig die ontwikkeld is op basis van het Qiy Afsprakenstelsel. Dit kan uw eigen app zijn die hiervoor wordt aangepast of een reeds bestaande app, zoals de app Dappre van Digital Me.

Stap 4 De Qiy QR-code kan tevens toegang bieden tot extra functionaliteit zoals een ‘download’ en ‘doorstuur’ -knop. Dit faciliteert individuen tevens om hun gegevens te downloaden of door te sturen.

Door de aansluiting op het Qiy Trust Framework kunnen individuen hun gegevens veilig opslaan in een van de aangesloten ‘personal clouds’ of kluizen.

Daarnaast kunnen gegevens onder regie van het individu eenvoudig en veilig beschikbaar worden gesteld aan andere partijen.

DIGITALME

de GDPR APP

Meer weten?

Neem contact op met **Maarten Louman**
+31 411 61 65 65
maarten.louman@digital-me.nl

1122d