CONSIDERATI
PARTNERS FOR THE DIGITAL WORLD

Statement Privacy Compliance iDIN

Om privacy optimaal te waarborgen binnen iDIN heeft Betaalvereniging Nederland Considerati gevraagd om iDIN op stelselniveau te toetsen aan privacywet- en -regelgeving.

Het stelsel zet door middel van '*Rules & Regulations*' (R&R) uiteen wat de verplichtingen zijn van de verschillende bij iDIN aangesloten partijen. Considerati heeft het stelsel getoetst aan de Wet bescherming persoonsgegevens en, waar relevant, de aankomende Algemene Verordening Gegevensbescherming. Individuele aangesloten partijen worden door de Betaalvereniging gecertificeerd volgens de R&R. De wijze waarop deze partijen zelf in concreto invulling aan de vereisten in de R&R geven is onderdeel van de certificering van deze partijen en valt vanwege de aard van het onderzoek buiten de scope van deze toets.

Hieronder volgen de belangrijkste bevindingen van Considerati:
De Betaalvereniging heeft gedegen aandacht besteed aan de privacy-aspecten die gemoeid zijn met het gebruik van iDIN door consumenten ('*privacy by design*'). Dit leiden wij af uit de door de Betaalvereniging opgestelde R&R, alsmede de openbare informatie op onder andere www.idin.nl en uit interviews met de Betaalvereniging. De verschillende privacy-aspecten zijn op stelselniveau goed ingericht.

Een aantal verduidelijkingen voor wat betreft bijvoorbeeld de verschillende rollen van partijen vanuit privacy-perspectief kunnen het stelsel nog verder verbeteren.

Het iDIN-stelsel biedt voldoende aanknopingspunten voor partijen binnen iDIN om de verschillende privacyaspecten te waarborgen. De verplichtingen die op de verschillende partijen op grond van toepasselijke privacy wet- en regelgeving rusten, zijn geadresseerd en geïmplementeerd in de *R&R*. Deze en de daaraan gekoppelde documenten besteden uitgebreid aandacht aan de verplichtingen die op iedere partij rusten, alsmede aan de wijze waarop de nakoming van die verplichtingen wordt gewaarborgd.

Zo stellen de R&R specifieke eisen aan de beveiliging van persoonsgegevens die in het kader van iDIN worden verwerkt. Ook wordt rekening gehouden met dataminimalisatie, door het beperken van persoonsgegevens die via iDIN kunnen worden opgevraagd en door pseudonimisering. Verder zijn datakwaliteit en bewaartermijnen geborgd in de R&R. De inrichting van het stelsel en de eisen die op stelselniveau aan de deelnemende partijen worden gesteld, zijn in lijn met de eisen uit de Wet bescherming persoonsgegevens.

Wij hebben een aantal aanvullende aanbevelingen geformuleerd om compliance van iDIN op stelsel-niveau nog verder te bevorderen. Zo bevelen we aan om de verdeling van rollen en verantwoordelijkheden specifiek met betrekking tot privacy helderder in de R&R voor iDIN vast te leggen. Deze aanbeveling wordt reeds door de Betaalvereniging opgevolgd. Verder verdient de uniforme communicatie over privacy in het kader van iDIN vanuit de verschillende bij iDIN betrokken partijen naar gebruikers toe onzes inziens nog aanvullende aandacht.

Samenvattend stellen wij vast dat iDIN op stelsel-niveau gebaseerd is op het principe van '*privacy by design*', zoals vereist in de aankomende Algemene Verordening Gegevensbescherming. Verder bieden de *R&R* voldoende aanknopingspunten voor partijen voor wat betreft privacy compliance. Onze laatste aanbevelingen om dit verder te bevorderen worden thans reeds door de Betaalvereniging uitgevoerd, waardoor privacy compliance op stelselniveau optimaal wordt gewaarborgd.