Informatie over de verwerking van persoonsgegevens binnen Digitale Cliënt Identificatie (DCI)

1. Inleiding

Notarissen kunnen gebruikmaken van het systeem Digitale Cliënt Identificatie (DCI) om cliënten digitaal te identificeren.

Deze informatie legt uit hoe persoonsgegevens binnen DCI worden verwerkt, welke partijen daarbij betrokken zijn en welke gegevens kunnen worden verwerkt wanneer u gebruikmaakt van DCI.

2. Wie is verantwoordelijk voor de verwerking van uw persoonsgegevens?

Wanneer een notaris gebruikmaakt van DCI om uw identiteit vast te stellen, is de betreffende notaris de verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming (AVG).

De notaris bepaalt:

- of DCI wordt gebruikt;
- voor welk doel DCI wordt ingezet;
- welke cliënt wordt uitgenodigd om zich via DCI te identificeren;
- welke persoonsgegevens noodzakelijk zijn voor de identificatie.

De Koninklijke Notariële Beroepsorganisatie (KNB) beheert en exploiteert het DCI-platform. Daarbij verwerkt de KNB persoonsgegevens uitsluitend namens en in opdracht van de notaris. De KNB treedt hierbij op als verwerker in de zin van artikel 4 lid 8 AVG.

3. Waarom wordt DCI gebruikt?

Notarissen zijn wettelijk verplicht de identiteit van cliënten vast te stellen en te verifiëren. Deze verplichtingen volgen onder meer uit:

- de Wet op het notarisambt (Wna);
- de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).

DCI ondersteunt notarissen bij het digitaal uitvoeren van deze identificatie- en verificatieverplichtingen.

DCI kan ook worden gebruikt door cliënten om zich te identificeren. Via DCI kunnen zij hun identiteitsgegevens veilig verstrekken aan de notaris.

4. Hoe werkt DCI?

Binnen DCI kunnen verschillende identificatiemethoden worden gebruikt.

Identificatie kan bijvoorbeeld plaatsvinden:

- via een elektronisch identificatiemiddel met een hoog betrouwbaarheidsniveau, zoals Itsme;
- door verificatie van een identiteitsdocument met behulp van technologie zoals ReadID.

Bij gebruik van een identiteitsdocument kunnen gegevens van het document en, indien beschikbaar, gegevens van de NFC-chip van het document worden gecontroleerd om de authenticiteit van het document vast te stellen.

De resultaten van deze controles worden beschikbaar gesteld aan de notaris zodat deze gebruikt kunnen worden voor identificatie en/of verificatie en vastgelegd kunnen worden in het dossier van de notaris.

5. Welke persoonsgegevens kunnen binnen DCI worden verwerkt?

Afhankelijk van de door de notaris gekozen identificatiemethode kunnen de volgende persoonsgegevens worden verwerkt.

Identificatiegegevens

- voornamen;
- achternaam;
- geboortedatum;
- geboorteplaats;
- geslacht;
- nationaliteit (indien beschikbaar via het gebruikte identificatiemiddel);
- BSN (indien beschikbaar via het gebruikte identificatiemiddel).

Gegevens van uw identiteitsdocument

- soort identiteitsdocument;
- documentnummer;
- land van afgifte;
- datum van afgifte;
- vervaldatum;

- pasfoto;
- handtekening.

Gegevens afkomstig van een elektronisch identificatiemiddel

Wanneer u zich identificeert met een elektronisch identificatiemiddel, zoals Itsme, kunnen identificatiegegevens worden verwerkt die door de aanbieder van dat identificatiemiddel worden verstrekt en bevestigd.

Resultaten van identiteits- en authenticiteitscontroles

Wanneer gebruik wordt gemaakt van verificatie van een identiteitsdocument, kunnen gegevens worden verwerkt over de uitkomst van controles die zijn uitgevoerd om de authenticiteit van het document vast te stellen. Daarbij kan worden vastgesteld of het document geldig lijkt en of er aanwijzingen zijn voor manipulatie van het document of de daarin opgenomen gegevens.

Technische gegevens

Voor het uitvoeren, beveiligen en beheren van DCI kunnen beperkte technische gegevens worden verwerkt, zoals log- en beveiligingsgegevens.

De exacte persoonsgegevens die worden verwerkt zijn afhankelijk van de identificatiemethode die de notaris kiest en van de gegevens die nodig zijn voor het identificatiedoel.

6. Wie heeft toegang tot de persoonsgegevens?

De persoonsgegevens die via DCI worden verwerkt zijn uitsluitend toegankelijk voor:

- het notariskantoor dat de identificatie heeft aangevraagd;
- daartoe bevoegde functioneel en technisch beheerders van de KNB voor zover dit noodzakelijk is voor beheer, onderhoud, beveiliging of probleemoplossing van het systeem.

De toegang van beheerders is beperkt tot hetgeen noodzakelijk is voor hun werkzaamheden en vindt plaats onder passende beveiligingsmaatregelen en geheimhoudingsverplichtingen.

7. Inzet van dienstverleners bij DCI

Voor het beheer, onderhoud en de beveiliging van DCI maakt de KNB gebruik van gespecialiseerde dienstverleners.

Voor identificatie- en verificatiediensten binnen DCI wordt onder meer gebruikgemaakt van diensten van Signicat. Daarbij kunnen tevens door Signicat ingeschakelde dienstverleners worden ingezet voor hosting, technische ondersteuning en verificatiediensten.

Voor zover deze dienstverleners persoonsgegevens verwerken, gebeurt dit uitsluitend onder passende contractuele afspraken en beveiligingsmaatregelen.

8. Beveiliging van persoonsgegevens

De KNB heeft passende technische en organisatorische maatregelen getroffen om persoonsgegevens binnen DCI te beschermen tegen verlies, onbevoegde toegang, wijziging of openbaarmaking.

Deze maatregelen omvatten onder meer toegangsbeveiliging, autorisatiebeheer, logging en monitoring, versleuteling van gegevens en beveiligingsmaatregelen voor systeembeheer.

De informatiebeveiliging van de KNB en haar dienstverlening, waaronder DCI, is ingericht volgens internationaal erkende normen voor informatiebeveiliging. De KNB beschikt over een ISO/IEC 27001-certificering voor haar informatiebeveiligingsmanagementsysteem. De certificering wordt periodiek onafhankelijk getoetst.

De beveiligingsmaatregelen worden regelmatig geëvalueerd en waar nodig aangepast.

9. Bewaartermijnen

Persoonsgegevens die via DCI worden verwerkt worden niet langer bewaard dan noodzakelijk voor het identificatieproces.

In beginsel geldt:

- nadat de identificatie is voltooid en de gegevens door de notaris zijn opgehaald, worden de gegevens na 10 dagen verwijderd;
- indien de gegevens niet door de notaris worden opgehaald, worden deze na 28 dagen verwijderd.

De notaris kan vervolgens zelf wettelijke bewaartermijnen hanteren voor gegevens die binnen het notariskantoor worden verwerkt.

10. Doorgifte buiten de Europese Economische Ruimte

Persoonsgegevens worden in beginsel verwerkt binnen de Europese Economische Ruimte (EER). Voor bepaalde ondersteunende diensten kunnen persoonsgegevens worden verwerkt in landen waarvoor de Europese Commissie heeft vastgesteld dat een passend beschermingsniveau voor persoonsgegevens geldt. Indien persoonsgegevens buiten de EER worden verwerkt, worden passende waarborgen toegepast overeenkomstig hoofdstuk V van de AVG.

11. Uitoefening van uw privacyrechten

Omdat de notaris verwerkingsverantwoordelijke is voor de verwerking van uw persoonsgegevens binnen DCI, kunt u voor vragen over uw persoonsgegevens en voor de uitoefening van uw rechten terecht bij uw notaris.

Dit betreft onder meer verzoeken inzake:

- inzage;
- rectificatie;
- verwijdering;
- beperking van verwerking;
- overdraagbaarheid van gegevens;
- bezwaar tegen verwerking.

De KNB ondersteunt notarissen waar nodig bij de afhandeling van dergelijke verzoeken.

12. Vragen of klachten

Voor vragen over de verwerking van uw persoonsgegevens binnen DCI kunt u contact opnemen met uw notaris.

Notarissen kunnen voor vragen over het functioneren of de beveiliging van DCI contact opnemen met de KNB .

Koninklijke Notariële Beroepsorganisatie (KNB)
Spui 184
2511 BW Den Haag
Telefoon: 070 330 7111

Functionaris voor Gegevensbescherming
E-mail: fg@knb.nl

Wanneer u van mening bent dat persoonsgegevens onjuist worden verwerkt, kunt u daarnaast een klacht indienen bij de Autoriteit Persoonsgegevens via www.autoriteitpersoonsgegevens.nl.

Versie 11 juni 2026