

Waarom dit leaflet?

In 2020 introduceerde de Europese Unie de EU-datastrategie, die Europa moet positioneren als voorloper in een datagedreven wereld. Deze strategie, deels al in werking, wordt vanaf 2026 volledig verplicht. Het doel is een uniforme data-economie – een Europese datamarkt – die innovatie stimuleert, data-uitwisseling vergemakkelijkt en de digitale soevereiniteit van de EU versterkt. Binnen deze markt kan data vrij circuleren tussen lidstaten en sectoren, wat voordelen biedt voor bedrijven, onderzoek en de publieke sector.

Sinds 2021 zijn er al complexe regels ingevoerd om dit doel te ondersteunen. Voor organisaties brengt deze wetgeving aanzienlijke uitdagingen met zich mee: juridische, marketing-, operations- en IT-teams moeten samenwerken om aan alle eisen te voldoen. Omdat deze vertaalslag tussen disciplines niet eenvoudig is, heeft Doccle dit leaflet ontwikkeld om inzicht te geven in de nieuwe regelgeving.

Sinds de wereld is gaan digitaliseren is klant-communicatie complex geworden.
Voor zowel de eindklant, die administratief geen overzicht meer heeft, als voor organisaties.



In dit leaflet zijn de volgende onderwerpen uitgewerkt:

Onderwerp	Pagina
1. Waarom de Europese Data strategie en wat moet het opleveren?	3
2. Breakdown van de belangrijkste onderdelen en de samenhang	3
3. EU Data strategie: wat zijn de wetten en wie controleert?	5
4. Overzicht van EU-Wetgevingen en Toepassingsgebieden: Privaat of Publiek	6
5. Wetgevingen per sector	7
6. Toelichting controlerende instanties	8
7. Ontzorgen op uitspraken en wetten Kifid, eIDAS 2.0, FiDa en anderen	10
8. DataWallets - DataSluizen en DataKluizen – Overeenkomsten en verschillen	15

Doccle ontzorgt en verbindt in Klantcommunicatie

Doccle is schaalbaar platform voor veilige klantcommunicatie, voor de prijs van een digitale

postzegel. Hiermee zijn we de digitale versie van PostNL voor het archiveren, versturen (CCM) en aantoonbaar afleveren van digitale documenten. Papier is ook een mogelijk output kanaal.

De bewezen geïntegreerde, veilige infrastructuur bestaat sinds 2014, heeft 3,8 miljoen geregistreerde eindgebruikers en 17.000 organisaties, waaronder de Belgische berichtenbox, De Goudse, de gemeente Rotterdam, NN, Allianz en KBC (geïntegreerd in Mijn-omgevingen en apps).

Kort samengevat: Doccle is de digitale verbindingslaag tussen uw systemen en uw klant – veilig, aantoonbaar en zonder extra complexiteit. We verbeteren klantcommunicatie, beperken het aantal applicaties en kunnen TCO kosten tot 50 % verminderen.

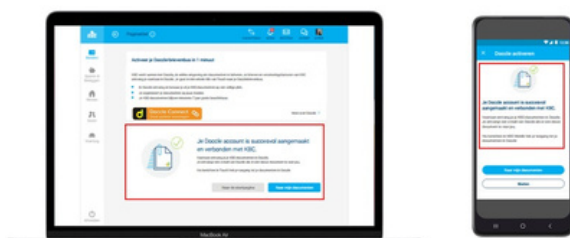
Klanten en partners zoals Univé, ANVA, Keylane en CCS zijn enthousiast over Doccle omdat het klant-communicatie structureel verbetert, governance- en compliancekosten verlaagt en de druk op IT-landschappen vermindert.

Doccle; Voor organisaties die top of mind willen blijven, een volle IT-kalender hebben en veilig willen communiceren. Dit levert concreet:

- Digitale kanaalgebruik: +30% meer traffic naar apps en digitale kanalen.
- Call reductie: -57% minder klantvragen door heldere en tijdige communicatie.
- Verhoging NPS: +15 punten door betere en veiligere klantinteractie.

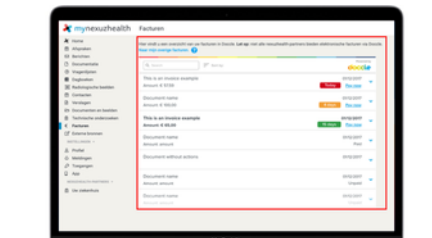
Sinds 2014 zijn er meer dan 3.500.000 gebruikers en meer dan 17.000 aangesloten organisaties met onder andere een overheids berichten box, geïntegreerd met een zeer grote bank (KBC) en patiëntenportalen.

Doccle geïntegreerd in KBC betaalomgeving



Meer ruimte voor online innovatie

Geïntegreerd in patiëntendossier van MyNexus health



Eenvoudig eigen bijdrage verrekenen

Door de API-first benadering is het eenvoudig en veilig om te koppelen en kan je als organisatie klein starten en doorgroeien in gebruik zodat je minder losse IT-applicaties nodig hebt.

Bij Doccle - communicatie en datadeel platform stelt de gebruikers en organisaties dagelijks in staat om makkelijk en veilig te communiceren aan deze regelgeving te voldoen.

In deze leaflet delen we onze kennis om inzicht te bieden in de nalegingsvereisten en hoe organisaties deze kunnen aanpakken. Voor belangrijke onderdelen van de wetgeving bieden we bovendien gecertificeerde oplossingen waarmee organisaties kosten en complexiteit kunnen beperken door het Doccle-platform in te zetten.

Doccle ontzorgt op het gebied van Kifid uitspraken, eIDAS 2.0, Financial Data Access (soort PSD2 voor financiële sector), en integreert met data wallets voor identificatie en data uitwisseling.

1. Waarom de Europese Data strategie?

In een wereld waar het datalandschap momenteel gedomineerd wordt door grote platforms uit de VS en China, biedt de Europese Commissie een alternatief dat strookt met Europese waarden zoals transparantie, vertrouwen en controle. De strategie richt zich op data-soevereiniteit, waarbij zowel bedrijven als individuen de controle krijgen over hun eigen data en rechtmatig kunnen profiteren van de waarde die deze data creëert.

Nieuwe benadering van datadeling

De Europese datasoevereinen vormen een cruciaal onderdeel van deze strategie. Deze ecosystemen, die gebaseerd zijn op vertrouwen, stellen deelnemers in staat om op een transparante, veilige en soepele manier data te delen, terwijl ze de volledige controle over hun data behouden. Dit opent nieuwe mogelijkheden voor data-deling tussen verschillende sectoren en lidstaten maar ook nieuwe innovatiemogelijkheden en kosten besparing voor organisaties.

Sinds 2020 heeft de Europese Commissie vijf belangrijke wetten ingevoerd om deze strategie uit te voeren. Zo bevordert de Data Governance Act het hergebruik van publiekelijk beheerde data en stimuleert de Data Act eerlijkheid binnen het digitale ecosysteem. Samen met de Digital Markets Act en de Digital Services Act bieden deze wetten een solide kader voor een eerlijke en transparante datamarkt in de EU. Wetgeving die hieruit voortvloeien zijn onder andere FiDa en eIDAS 2.0.

FiDa (Financial Data Access) is te vergelijken met PSD2 maar dan voor gehele Financiële sector. eIDAS 2.0 brengt vertrouwen in digitale communicatie terug met echt te vertrouwen communicatiekanalen, herleidbaarheid van data en documenten en identificatie van de persoon (eindklant) en de organisatie.

2. Breakdown van de belangrijkste componenten en de samenhang:

1. Doelstellingen van de Europese datastrategie

- Versterken van de digitale interne markt: Creëren van een geïntegreerde digitale economie waarin data vrij tussen landen en sectoren kan circuleren.
- Data-soevereiniteit: Waarborgen dat data-eigenaarschap en -beheer binnen de EU blijft, en dat Europese burgers en bedrijven controle behouden over hun data.
- Innovatie bevorderen: Door data beter beschikbaar te maken voor bedrijven en overheden, worden innovaties in sectoren zoals gezondheidszorg, energie en financiën gestimuleerd.

2. Belangrijkste pijlers

- Data Governance Act (DGA): Regelt de voorwaarden waaronder data beschikbaar kan worden gesteld voor secundair gebruik, met name door overheden en publieke instellingen. Deze wet creëert een kader voor data-uitwisseling en stimuleert vertrouwen in datadeling tussen organisaties.

- Data Act: Richt zich op data-eigendom en stelt regels op voor toegang tot data door derde partijen. Het doel is om eerlijkere concurrentie te creëren, waarbij kleine bedrijven makkelijker toegang krijgen tot data van grotere spelers.
- Open Data Directive: Bevordert het hergebruik van publieke data door bedrijven, zodat deze data vrij en herbruikbaar beschikbaar wordt gesteld voor innovatie.

3. Sectorale Data Ruimtes

- Financiële data (FiDa): Bevordert de veilige uitwisseling van financiële data tussen banken, verzekeraars en consumenten, met als doel de transparantie te vergroten en de concurrentie te stimuleren.
- Gezondheidsdata: De European Health Data Space ondersteunt de veilige uitwisseling van gezondheidsdata, bevordert grensoverschrijdende samenwerking en versterkt gezondheidszorginnovatie.
- Energie- en klimaatdata: Ruimtes voor data uit de energiesector zijn ontworpen om data-uitwisseling te bevorderen die de energietransitie versnelt, en oplossingen zoals slimme meters en duurzaam energiebeheer te ondersteunen.

4. Technische infrastructuur

- Cloud en data-infrastructuren: Initiatieven zoals GAIA-X stimuleren het gebruik van veilige, Europese cloud-oplossingen die voldoen aan EU-regels voor privacy en veiligheid.
- Interoperabiliteit: De strategie bevordert standaarden die ervoor zorgen dat data tussen verschillende systemen en sectoren kan worden gedeeld, zonder technische obstakels.

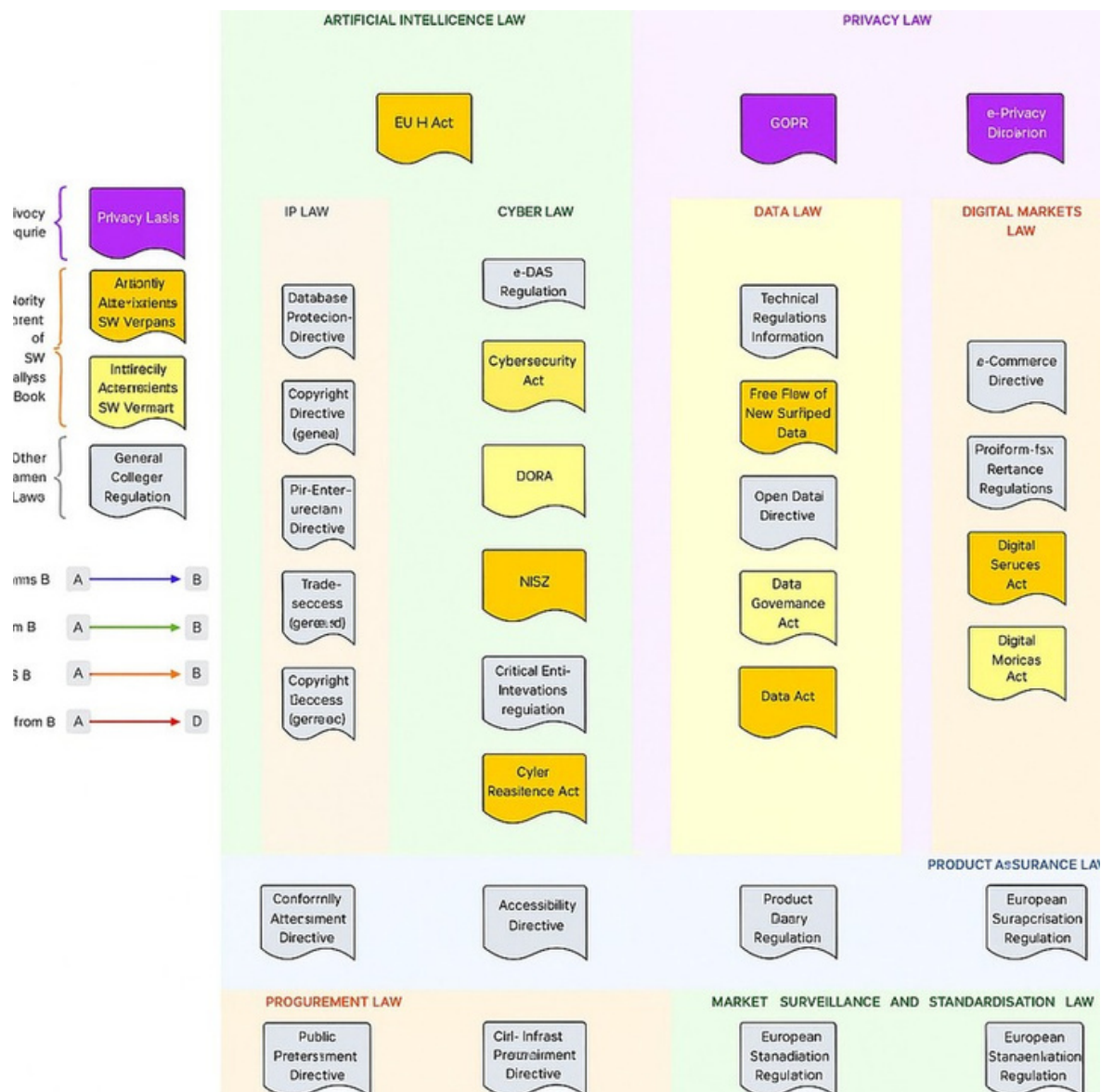
5. Data Soevereiniteit en Vertrouwensregels

1. Privacybescherming (GDPR): De bescherming van persoonlijke data blijft een centraal onderdeel, waarbij gebruikers expliciet toestemming moeten geven voor het delen van hun gegevens.
2. Digitaal vertrouwen (eIDAS 2.0): Nieuwe regels rond elektronische identificatie en vertrouwensdiensten, die zorgen voor veilige en betrouwbare digitale interacties tussen burgers, bedrijven en overheden.

De Europese datastrategie integreert regelgeving (zoals de Data Governance Act en GDPR) met technische infrastructuren en sectorale initiatieven (zoals de financiële - en gezondheids datasectoren) om een gestroomlijnde data-economie te creëren. Hierdoor wordt data veiliger, efficiënter en innovatiever benut. Het uiteindelijke doel is dat data-uitwisseling bijdraagt aan economische groei en soevereiniteit, terwijl privacy en gebruikerscontrole centraal blijven staan.

Deze aanpak legt de basis voor een veilige en concurrerende digitale markt in Europa.

De grafische weergave van de Europese Data Strategie:



Bron: Zoltan Precsenyi – Director of Privacy

De komende **#DigitalOmnibus** van de EU leidt nu al tot gepassioneerde debatten. Of je er nu naar uitkijkt met hoop en verwachting of angst en twijfel, hier is mijn overzicht van het regelgevingslandschap waar we naar kijken. Vereenvoudiging is zonder meer wenselijk, maar of zelfs het stroomlijnen van dit niveau van complexiteit daadwerkelijk haalbaar is, valt nog te bezien. In ieder geval, om volgende week op **#IAPP #DPC2025** te begrijpen hoe we hier zijn gekomen en om te zien waar we naartoe gaan, bekijk het panel over "Data Democracy to Digital Anarchy", met **Cynthia Cole**, **Elizabeth Denham CBE** en **Ilias Chantzios**.

3. EU Data strategie: wat zijn de wetten en wie controleert?

Toelichting per wetgeving:

1. AI Act: De AI Act heeft brede implicaties voor sectoren die kunstmatige intelligentie gebruiken, zoals verzekeringen, waar AI wordt ingezet voor risicobeoordeling en claimsbeheer. Andere sectoren zoals banken en telecom kunnen eveneens aan de wetgeving onderhevig zijn, vooral als AI-toepassingen persoonlijke data verwerken of kritieke beslissingen beïnvloeden.
 2. Cybersecurity Act: Deze wetgeving richt zich op het versterken van cyberbeveiliging via certificeringskaders voor producten, diensten en processen in alle relevante sectoren, inclusief verzekeringen en waterleidingbedrijven.
 3. Data Governance Act: Deze wet bevordert datadeling en governance en is gericht op sectoren waar het beheer van grote hoeveelheden data essentieel is, zoals in de verzekeringsbranche en salarissen.
 4. DGA (Data Governance Act): In de tabel is een duplicaat van de Data Governance Act opgenomen, wat aangeeft dat de meeste sectoren zich moeten richten op gegevensuitwisselingsnormen. Alleen telecom heeft een beperktere directe verplichting.
 5. eIDAS 2.0: Deze wetgeving reguleert digitale identificatie en elektronische vertrouwensdiensten, wat van belang is voor alle sectoren die elektronische handtekeningen en veilige digitale interacties vereisen.
 6. FiDA (Financial Data Access): FiDA is gericht op de financiële sectoren zoals verzekeringen en banken, waar de toegang tot financiële gegevens cruciaal is voor diensten zoals kredietwaardigheidstoetsen en advies.
 7. GDPR (AVG): De GDPR geldt voor alle sectoren die persoonsgegevens verwerken, wat de meeste sectoren in de tabel betreft.
 8. NIS2: Deze richtlijn is gericht op de beveiliging van netwerk- en informatie-infrastructuur en omvat meerdere sectoren met essentiële diensten, waaronder verzekeringen en waterleidingbedrijven.
 9. DORA: De wetgeving richt zich specifiek op financiële instellingen zoals banken en verzekeraars, met als doel hun operationele digitale veerkracht te waarborgen.
 10. DMA: De Digital Markets Act reguleert de macht van grote digitale platforms ("gatekeepers"), wat vooral relevant is voor banken en telecombedrijven die een dominante positie in de markt kunnen hebben.
 11. DSA: Deze wetgeving is gericht op digitale platforms en tussenpersonen, met name in de telecom- en banksector, die diensten leveren die betrekking hebben op online contentbeheer.
 12. Open Data Directive: De richtlijn is van toepassing op sectoren die gebruikmaken van openbare data, zoals pensioenfondsen en salarissen.
 13. PSD2: De betaalrichtlijn is van toepassing op banken en heeft betrekking op de toegang tot bankgegevens voor betaalinstanties en fintechbedrijven.
- Van de genoemde wetten is geen enkel een pure privacywet zoals de GDPR (General Data Protection Regulation). Deze wetten richten zich voornamelijk op andere aspecten van digitale regelgeving zoals marktregulering, data governance, en digitale identificatie, maar hebben wel indirecte implicaties voor privacybescherming.

4. Overzicht van EU-Wetgevingen en Toepassingsgebieden: Privaat of Publiek

EU-Wetgeving	Focus van de wetgeving	Focus	Actief vanaf	Gehandhaafd Cor	trolerende instantie
AI Act	Regulering van AI-toepassingen	Publiek & Privaat	Verwacht in 2025-2026	Verwacht in 2026-2027	Europese Commissie
Cybersecurity Act	Certificering van cyberveiligheid	Publiek & Privaat	27 juni 2019	27 juni 2019	ENISA & Nationale cybersecurity-autoriteiten
Data Governance Act	Governance van datauitwisseling	Publiek & Privaat	24 september 2023	Verwacht in 2024	Nationale toezichthouders & Europese Commissie
DMA(Digital Markets Act)	Regels voor digitale markten	Privaat	2 mei 2023 17 januari	25 maart 2024	Europese Commissie
DORA (Digital Operational Resilience Act)	Operationele digitale veerkracht	Privaat	2025	Verwacht in 2025	Europese Centrale Bank (ECB) & ESAs
DSA (Digital Services Act)	Regels voor digitale diensten	Privaat	16 november 2022	17 februari 2024	Europese Commissie & Nationale toezichthouders
eIDAS	Digitale identificatie en vertrouwen	Publiek & Privaat	Verwacht in 2024-2025	Sinds 2018, aangescheppt per 2025-2026	Nationale toezichthouders & Europese Commissie
FiDA (Financial Data Access)	Toegang tot financiële data	Publiek & Privaat	Verwacht in 2025-2026	Verwacht in 2026	Europese Bankenautoriteit (EBA) & ESMA
GDPR (General Data Protection Regulation)	Gegevensbescherming en privacy	Publiek & Privaat	25 mei 2018	25 mei 2018	Nationale gegevensbeschermings autoriteiten
NIS2	Cybersecurity en netwerkbeveiliging	Publiek & Privaat	18 oktober 2024	18 oktober 2024	Nationale cybersecurity-autoriteiten
Open Data Directive	Hergebruik van overheidsdata	Publiek	17 juli 2021	17 juli 2021	Nationale en Europese overheidsinstellingen
PSD2	Betaaldiensten en toegang	Privaat	13 januari 2018	13 januari 2018	Nationale toezichthouders & Europese Centrale Bank (ECB)

5. Wetgevingen per sector

EU-Wetgeving	<i>Banken</i>	<i>Verzekeren</i>	<i>fonds Pensioen -</i>	<i>Beveiliging - Uitvoering</i>	<i>Telecom</i>	<i>Salaris verwerkers</i>	<i>Overheid</i>
AI Act	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Cybersecurity Act	Ja	Ja	Ja	Ja	Ja	Ja	Ja
DGA Data Governance Act	Ja	Ja	Ja	Ja	Ja	Ja	Ja
eIDAS 2.0 *	Ja	Ja	Ja	Ja	Ja	Ja	Ja
FiDA (Financial Data Access)	Ja	Ja	Ja	Ja	Nee	Nee	Nee
GDPR (General Data Protection Regulation)	Ja	Ja	Ja	Ja	Ja	Ja	Ja
NIS2	Ja	Ja	Ja	Ja	Ja	Ja	Ja
DORA Digital Operational Resilience Act	Ja	Ja	Nee	Nee	Nee	Nee	Nee
DMA (Digital Markets Act) *	Ja	Nee	Nee	Nee	Ja	Nee	Nee
DSA (Digital Services Act) *	Ja	Nee	Nee	Nee	Ja	Nee	Nee
Open Data Directive *	Ja	Nee	Ja	Ja	Ja	Ja	Ja
PSD2	Ja	Nee	Nee	Nee	Nee	Nee	Nee

*)De wetten DSA, DMA, DGA, DA en eIDAS hebben betrekking op verschillende aspecten van digitale regelgeving, maar ze zijn niet allemaal strikt privacywetten.

Hier is een overzicht:

1. DSA (Digital Services Act):

Publiek & Privaat - Nietspecifieke privacywet

: De DSA is gericht op het reguleren van _____

digitale diensten en platforms. Het legt verantwoordelijkheden op voor het beheer van illegale inhoud, transparantie van advertenties, en bescherming van gebruikers, maar heeft niet als primaire focus de bescherming van persoonlijke gegevens. Het heeft echter wel enkele implicaties voor privacy, vooral in verband met de transparantie van gebruikersgegevens en het beheer ervan door platforms.

2. DMA (Digital Markets Act):

Niet een privacywet: De DMA richt zich op het reguleren van grote digitale platforms (de zogeheten “gatekeepers”) om eerlijke concurrentie op digitale markten te waarborgen. Het doel is om machtsmisbruik door dominante platforms te voorkomen. Hoewel dit indirect invloed kan hebben op privacy, richt de DMA zich vooral op marktregulering en concurrentie.

3. DGA (Data Governance Act):

Niet specifiek een privacywet: De DGA richt zich op het faciliteren van data-uitwisseling en het bevorderen van een Europese datastrategie. Het legt regels vast voor het hergebruik van beschermde data, de oprichting van dataruimtes, en het stimuleren van datadeelplatforms. Het is meer gericht op data governance en het stimuleren van de datamarkt dan op privacybescherming.

4. DA (Data Act):

Niet specifiek een privacywet: De Data Act heeft als doel om het gebruik en delen van data in de EU te bevorderen, met regels die de rechten van bedrijven en consumenten op data beschermen. Het richt zich op data-eigendom en toegang tot data, vooral in de context van IoT-apparaten en andere digitale ecosystemen. Hoewel de Data Act zeker gevolgen heeft voor privacy, is het geen wet die zich uitsluitend richt op privacybescherming.

5. eIDAS (Electronic Identification, Authentication and Trust Services):

Niet een privacywet, maar wel relevant voor privacy: eIDAS gaat over digitale identificatie en het creëren van een betrouwbare digitale omgeving in Europa. Het richt zich op het veilig en betrouwbaar beheren van digitale identificatie en elektronische transacties. Hoewel eIDAS cruciaal is voor de veiligheid van digitale identificatie en authenticatie, is het geen privacywet per se. Het ondersteunt echter de bescherming van persoonlijke gegevens door veilige identificatie diensten te reguleren.

6. Toelichting controlerende instanties:

1. AI Act: De Europese Commissie is verantwoordelijk voor de implementatie en toezicht op de naleving van de AI-wetgeving.
2. Cybersecurity Act: De European Union Agency for Cybersecurity (ENISA) werkt samen met nationale autoriteiten om naleving te waarborgen.
3. Data Governance Act (DGA): Zowel nationale toezichthouders als de Europese Commissie houden toezicht op de naleving.
4. DMA: De Europese Commissie is de primaire toezichthouder voor grote platforms die worden aangeduid als "gatekeepers".
5. DORA: Toezicht wordt uitgevoerd door de Europese Centrale Bank (ECB) en Europese Toezichthoudende Autoriteiten (ESAs).
6. DSA: Zowel de Europese Commissie als nationale toezichthouders zijn betrokken bij het toezicht, afhankelijk van de schaal en de aard van de digitale diensten.
7. eIDAS 2.0: Nationale toezichthouders en de Europese Commissie zorgen samen voor naleving van de regelgeving.
8. FiDA: De Europese Bankenautoriteit (EBA) en de European Securities and Markets Authority (ESMA) zijn de belangrijkste toezichthouders.
9. GDPR: Nationale gegevensbeschermingsautoriteiten handhaven de AVG in elk EU-lidstaat.
10. NIS2: Nationale autoriteiten houden toezicht op de naleving van deze richtlijn, gericht op netwerk- en informatiebeveiliging.
11. Open Data Directive: Nationale en Europese instanties waarborgen de toepassing van deze richtlijn.
12. PSD2: Nationale toezichthouders en de Europese Centrale Bank (ECB) handhaven de naleving van de betalingsrichtlijn.

Toelichting:

- * ESAs: Europese Toezichthoudende Autoriteiten, zoals EBA, EIOPA, en ESMA.
- ** Handhaving van DMA-richtlijnen begon in maart 2024
- *** ESMA: European Securities and Markets Authority.
- **** ENISA: European Union Agency for Cybersecurity.

Bronnen:

17February2024:TheDigital ServicesAct(DSA)isnowfullyapplicable - OsborneClarke | Osborne Clarke | (<https://www.osborneclarke.com/insights/17-february-2024-digital-services-act-dsa-now-fully-applicable>)

TheDigital ServicesActIsNow Fully ApplicableAndEnforceable - SocialMedia - Media, Telecoms, IT,Entertainment-United States(<https://www.mondaq.com/unitedstates/social-media/1430942/the-digital-services-act-is-now-fully-applicable-and-enforceable>)

Digital Services Act – EU Digital Services Act (DSA) – Official Text & Resources <https://dsa-info.eu>

7. Ontzorgen op uitspraken en wetten Kifid, eIDAS 2.0, FiDa etc.

‘Rechtsgeldige digitale communicatie door vertrouwen in en rechtskracht te creëren in uitwisseling van digitale documenten en data’

Om de consument en MKB-er te beschermen zijn er vanuit Europa en Nederlandse tal van wetgevingen gemaakt rond eIDAS2.0, Open Data, Open Insurance, FiDa, Dora etc. Deze zijn deels al van kracht komen de komende twee jaar in sneltreinvaart op organisaties af. Deze wetten stellen strikte eisen rond klant identificatie, toestemming voor data uitwisseling en data minimalisatie, audittrails, open standaarden etc.

Ontwikkeling & wetgeving	Toelichting	Doccle ontzorgt
Kifid uitspraken Financiële instellingen	De verzender moet kunnen aantonen dat het bericht is verstuurd en is afgeleverd: De Klant niet meer verantwoordelijk maken om op zoek te gaan naar informatie: ‘ <i>Mijn Omgeving en email zijn niet genoeg voor goede klant communicatie</i> ’	
Kifid nr. 2024-0125 Actief: 12-2-2024	- Mijn-omgeving is passief kanaal - e-mail is onveilig: Phishing risico, niet beveiligd kanaal, data in mailboxen vaak geen eigendom van gebruiker - Afleveren met post is veilige optie	Polissen, voorwaarden, facturen en groene kaart kunnen worden afgeleverd in persoonlijke kluis incl. leesbevestiging. Digitaal of voor wie wil printen op papier.
Kifid nr. 2024-0157 Actief: 12-2-2024	- Mijn-omgeving is passief kanaal - e-mail is onveilig: Phishing risico, niet beveiligd kanaal, data in mailboxen vaak geen eigendom van gebruiker - Afleveren met post is veilige optie	Polissen, voorwaarden, facturen en groene kaart kunnen worden afgeleverd in persoonlijke kluis incl. leesbevestiging. Digitaal of voor wie wil printen op papier.
eIDAS 1.0 NL overheidsorganisaties en private organisaties met een publieke taak Actief: 26-9-2018 Identificatie- en authenticatiemiddelen	Stelt eisen aan elektronische identificatie- en authenticatiemiddelen omwille van veiligheid, betrouwbaarheid en het mogelijk maken van grensoverschrijdend gebruik	
	Criteria bij communicatie: (Q)eSignature, (Q)eSeal, (Q)eTimestamp, QWAC, (Q)ERDS Bijvoorbeeld DigiD, eHerkenning	Doccle voldoet hier sinds 2020 aan. Belgische berichtenbox is sinds 2017 met Doccle gekoppeld. Bezoek naar BE berichtenbox nam met 40 % toe.
eIDAS 2.0 Overheidsinstanties en private organisaties zoals banken, verzekeraars, pensioenuitvoerders, e-commerce platformen Actief: medio 2026	Vertrouwen in en rechtskracht creëren in uitwisseling van digitale documenten en data <i>‘Een gekwalificeerde elektronische attestering van attributen heeft dezelfde rechtsgevolgen als wettelijk uitgegeven attesteringen op papier’ (eIDAS artikel 45 bis)</i>	

Ontwikkeling & wetgeving	Toelichting	Doccle ontzorgt
Uitbreiding trust services:	Zoals Elektronische handtekeningen, Echtheidszegels, Tijdstempels.	Timestamp van het ingaande en uitgaande dataverkeer
Elektronische identificatie (Q)eID	Elektronische identificatie (eID) is een cruciaal element bij het waarborgen van de veiligheid en beveiliging van digitale transacties. Het dient als een digitaal identiteitsbewijs, waardoor individuen toegang hebben tot online diensten, elektronische transacties kunnen uitvoeren en communiceren met overheidsplatforms met een hoger niveau van vertrouwen. Digitaal tekenen, gekwalificeerde eSigs hebben dezelfde wettelijke waarde als een natte handtekening	Persoonsidentificatie op Verschillende niveaus van betrouwbaarheid ondersteund: 1. Laag 2. eIDAS hoog
Digitaal ondertekenen (Q)eSignature		Digitaal ondertekenen wordt op verschillende niveau's van betrouwbaarheid ondersteund: 1. Laag 2. Substantieel 3. eIDAS hoog
Garanderen herleidbaarheid van elektronische documenten (Q)eSeal	Zorgt voor herleidbaarheid van elektronische documenten om herkomst en integriteit te garanderen: - Ongekwalificeerd - Geavanceerd - Gekwalificeerd	Op alle levels van assurance kunnen documenten en data worden ontvangen en herleidbaar geïdentificeerd. Doccle slaat de ge-eSealde documenten op. De eSeal wordt gezet door leverancier naar keuze van de klant.
Tijdstip koppelen aan elektronisch document (Q)eTimestamp	Koppelt een elektronisch document (zoals inkooporder) aan een bepaald tijdstip	Alle ontvangen documenten en data worden voorzien van specifiek datum/ tijdstip. Doccle gebruikt deze eTimestamp in het kader van elektronische handtekeningen. Het timestampen van documenten of attributen is geen afzonderlijk afneembare dienst. Doccle voorziet documenten en data wel van een timestamp, maar niet qualified herleidbare attributen. Verschillende niveaus worden ondersteund:
Bewijs van verzending en levering (Q)eRDS	Elektronische aflevering van gegevens. Levert een bewijs van verzending en levering.	1. Gelezen 2. Read & accept 3. Digitaal ondertekend 4. Aangetekend ontvangen
Bevestigen van gegevens (Q)EAA	Een attestatie in elektronische vorm die authenticatie van attributen mogelijk maakt (zoals nationaliteit of rijvaardigheid)	Data en attributen worden geattesteerd. Her-qualified attesteren is nog niet mogelijk.
Betrouwbaar digitaal archief (Q)eArchiving	Service voor digitaal archiveren, behoud van integriteit en garanderen van herkomst	Legal archive voldoet aan eIDAS 2.0 wetgeving. Doccle wacht op certificering volgens eIDAS 2.0

Ontwikkeling & wetgeving	Toelichting	Doccle ontzorgt
Verzekeren accuraatheid gegevens (Q)eLedgers	Reeks aan elektronische data die integriteit en accuraatheid verzekerd (blockchain)	Integrale werking Doccle: herleidbare en niet te wijzigen data (attributen en documenten)
Remote ondertekenen en sealen voor persoon (Q)ESCD	Managen van remote (Q)eSig/(Q)eSeal door een QTSP voor een persoon	Hier vervult Doccle geen rol in
Certificaten betrouwbare website (Q)WAC	Elektronische certificaten die bewijzen dat een website betrouwbaar is	Hier vervult Doccle geen rol in
Financial Data Access (FIDA)	Te vergelijken met PSD2 wetgeving maar dan voor financiële/ administratieve data.	
Financiële dienstverleners zoals banken, pensioenuitvoerders, verzekeraars (exclusief leven en overlijden), beleggingsmaatschappijen	Regels voor het delen van klantgegevens in de financiële sector voor elke EU Lidstaat. Klanten meer controle geven over eigen gegevens door hun gegevens op een veilige manier te delen. De klant kan hierdoor een breder gamma van betere en goedkopere financiële producten en diensten kan verkrijgen.	Doccle is bestempeld als een actief communicatiekanaal. KBC gebruikt Doccle om deze reden voor al hun wettelijk verplichte communicatie die niet louter via passieve kanalen (mijn-Omgeving) of email mogen gestuurd worden
Sterke authenticatie	Voor toegang tot financiële gegevens is sterke authenticatie vereist om ongeautoriseerde toegang te voorkomen.	Doccle kan organisaties ontzorgen omdat zij sterke authenticatiemethode voor veilige toegang.
Data delen binnen financiële sector en over sectoren	Financiële gegevens kunnen worden gedeeld tussen verschillende sectoren om betere diensten te leveren.	Doccle levert datadeling met data minimalisatie voor zowel data, documenten als profiel vragen binnen specifieke processen en over sectoren heen.
Toestemming vereist	Voor toegang tot financiële gegevens is expliciete toestemming van de gebruiker vereist.	Doccle ondersteunt in expliciet consent management inclusief een audittrail voor gebruikers en organisatie.
Gegevensbeveiliging	Financiële gegevens moeten veilig worden opgeslagen en verwerkt om de privacy van gebruikers te waarborgen.	Doccle kan een veilig platform bieden voor het opslaan en delen van financiële gegevens.
Transparantie	Gebruikers moeten duidelijk geïnformeerd worden over hoe hun financiële gegevens worden gebruikt en gedeeld.	Doccle kan transparantie bieden over het gebruik en de doeleinden van financiële gegevens.
Data-beleid	Er moeten duidelijke richtlijnen zijn voor het bewaren en verwijderen van financiële gegevens.	Doccle kan gebruikers helpen bij het beheren van hun data voorkeuren en het veilig verwijderen van gegevens.
AVG / GDPR	De wetgeving moet voldoen aan de algemene verordening gegevensbescherming (AVG).	
Toestemming	Gebruikers moeten expliciet toestemming geven voor het verzamelen en verwerken van hun persoonlijke gegevens.	Doccle biedt een veilig en transparant platform waar gebruikers met toestemming kunnen beheren en controleren en delen.

Ontwikkeling & wetgeving	Toelichting	Doccle ontzorgt
Dataminimalisatie	Alleen de noodzakelijke persoonsgegevens mogen worden verzameld en verwerkt voor het beoogde doel.	Doccle helpt bij het minimaliseren van gegevensverzameling en -verwerking door alleen relevante gegevens te gebruiken.
Recht op inzage	Gebruikers hebben het recht om te weten welke gegevens over hen worden verzameld en verwerkt, en om deze gegevens op te vragen.	Doccle kan gebruikers een gemakkelijke toegang bieden tot hun persoonsgegevens via een transparant portaal.
Recht op rectificatie	Personen hebben het recht om onjuiste persoonsgegevens te corrigeren.	Doccle stelt gebruikers in staat om correcties aan te brengen in persoonsgegevens. Op verzoek van een organisatie kan een gebruiker toestemming geven actuele gegevens te delen en zo gegevens te rectificeren en her te gebruiken. Doccle biedt de gebruiker de
Recht om vergeten te worden	Personen hebben het recht om hun persoonsgegevens te laten verwijderen.	mogelijkheid om persoonsgegevens veilig en permanent te verwijderen wanneer dit nodig is. Doccle kan helpen bij het
Datalekken	Organisaties moeten datalekken melden en adequate maatregelen nemen om de gelekte gegevens te beschermen.	detecteren en melden van datalekken, en bij het implementeren van beveiligingsmaatregelen om deze te voorkomen. Doccle levert een platform dat
Privacy by design	Privacy moet al bij het ontwerp van systemen en processen worden meegenomen, en niet achteraf worden toegevoegd.	vanaf de basis is ontworpen met privacy en gegevensbescherming in gedachten. Doccle ondersteunt gebruikers en aangesloten organisaties bij
Gegevensportabiliteit	Personen hebben het recht om hun persoonsgegevens over te dragen naar een andere dienstverlener.	het voldoen aan dit recht door het eenvoudig overdragen van persoonsgegevens naar andere systemen.
Communicatie wensen	Dilemma	
Outbound communicatie: Verstuurde Informatie wordt goed gelezen door ontvanger	Communicatie over Financiële diensten wordt over het algemeen beperkt gelezen. Outbound communicatie wordt vaak als kosten gezien	De leesgraad in Doccle blijkt hoger te zijn: • 30 % meer online traffic • NPS + 15 • Callverkeer -/- 57 %
Inbound communicatie: op de hoogte blijven van situatie bij de klant	Wijzigingen in de situatie van de eindklant worden nauwelijks doorgegeven: de drempel is hoog, de waarde voor de klant is beperkt. Hierdoor blijft CRM data beperkt actueel en is men beperkt op de hoogte van de klant situatie.	Via de digitale verbinding en het hergebruik van informatie wordt het eenvoudig om de hoogte te blijven van Actuele klant data. Zoals bijvoorbeeld op de hoogte blijven van (life) events.
Een goede servicegraad kunnen verlenen aan klanten	Veel organisaties verlenen ongeveer hetzelfde service niveau. Voor elke verbetering is IT inzet nodig. Deze capaciteit is vaak beperkt waardoor de servicegraad op hetzelfde niveau blijft.	Doccle heeft door de jaren heen generieke services ontwikkeld die het serviceniveau verbeteren. Klanten van Doccle

Ontwikkeling & wetgeving	Toelichting	Doccle ontzorgt
		hoevenzichzelf niet te ontwikkelen.
IT-kalender is niet belemmerend	Bij veel organisaties zijn de kalenders overvol en moet een zeer grote businesscase te onderbouwen worden overlegd om prioriteit te krijgen. Hierdoor kunnen veel verbeteringen niet worden uitgevoerd.	Doccle levert standaard API componenten om organisaties te ontzorgen en te ontlasten in de bestaande roadmap.
Governance processen verlopen soepel en veilig	Huidige governance processen zijn veelal volledig losgekoppeld van het proces rond de productaanvraag. Bijvoorbeeld KYC proces is losgekoppeld van aanvraag van hypotheek proces.	Vanuit één geïntegreerde flow wordt zowel product gelieerde als governance informatie worden uitgewisseld.
Papier- Digitaal integratie	Van niet iedere klant zijn de juiste digitale contact gegevens. Bijvoorbeeld deelnemers die in het buitenland wonen en waar geen mailadres van is	Via op papier geprinte QR codes kan een digitale verbinding met de organisatie worden gelegd. Hierna kunnen documenten en data overzichtelijk en veilig worden uitgewisseld. Via API worden omni-channel processen aangestuurd. Voor klanten die communicatie op papier willen blijven ontvangen kan Doccle het printwerk uit handen nemen.
Uitdaging organisatie		
Ontwikkeling en beheer	Veel aandacht gaat uit naar het stabiel en veilig houden van systemen en het beheer van bestaande applicaties. Ook implementeren van wet- en regelgeving kost veel aandacht.	Bewezen componenten kunnen met API koppelingen of widgets worden ingezet. Omdat Doccle het onderhoud op deze componenten verzorgd wordt de klantorganisatie hiermee ontlast.
Security	Organisaties en systemen moeten opener en flexibeler worden terwijl hackers en systemen van hackers in hoog tempo doorontwikkelen.	Doccle kent vanuit haar klanten zeer strikte governance regels en jaarlijks vele pentesten. Ze voldoet aan de hoogste security eisen om haar klanten veilig te bedienen.
Applicatie landschap	Door de veelheid van oplossingen is applicatielandschap veelal een lappendeken.	Vanuit één koppeling worden uiteenlopende deel oplossingen ondersteund. Het is mogelijk om klein te starten en stap voor stap door te groeien. Doccle ontzorgt zo organisaties
Data kwaliteit	Datakwaliteit door het niet op de hoogte blijven niet op de hoogte situatie klant.	Via de digitale verbinding en het hergebruik van informatie wordt het eenvoudig om de hoogte te blijven van Actuele klant data. Zoals bijvoorbeeld op de hoogte blijven van (life) events.

8. Ontzorgen op WMEBV- Wet Modernisering Elektronisch Bestuurlijk Verkeer

WMEBV vraagt om **betere digitale dienstverlening**.

Doccle verlaagd de drempel om dat **praktisch uitvoerbaar te maken**, zonder dat elke organisatie het wiel opnieuw hoeft uit te vinden.

Met de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) krijgen inwoners en ondernemers het recht om officiële berichten elektronisch aan gemeenten en andere overheidsorganisaties te versturen. Het gaat om berichten die bijvoorbeeld gaan over een aanvraag, beschikking, besluit, klacht of zienswijze. De Wmebv is een aanpassing op de Algemene wet bestuursrecht (Awb). Pilotgemeenten geven aan dat er ongeveer 400 verschillende types elektronisch verkeer zijn die straks moeten voldoen aan de Wmebv.

Bron: <https://vng.nl/wmebv>

De Wmebv kent 3 onderdelen:

- het **verzenden** van officiële berichten door inwoners en ondernemers
- het **ontvangen** van formele berichten door bestuursorganen
- **invulling geven** aan de zorgplicht om ondersteuning te bieden bij dienstverlening aan digitaal minder vaardige inwoners.

Wat moeten gemeenten regelen voor de Wmebv?

Gemeenten moeten voor de Wmebv het volgende regelen:

- Digitale kanalen aanwijzen die inwoners kunnen gebruiken bij het verzenden van officiële berichten over aanvragen, beschikkingen, besluiten, klachten of zienswijzen. En zorgen dat deze kanalen gebruiksvriendelijk zijn en voldoen aan de eisen van de Wmebv.
- Regelen dat er bij een binnengekomen elektronisch bericht van een inwoner of ondernemer een ontvangstbevestiging wordt verstuurd.
- Regelen dat er bij het plaatsen van een bericht in een 'berichtenbox' of MijnOmgeving een notificatie wordt verstuurd inclusief einddatum van de termijn waarbinnen gereageerd moet worden.
- In het geval de inwoner heeft aangegeven digitaal te willen communiceren en een notificatie of bericht kan digitaal niet afgeleverd worden aan de inwoner, geldt een inspanningsverplichting om op een andere manier contact op te nemen en de inwoner hierop wijzen.
- In het geval van een storing waarbij de reactietijd langer wordt, is de gemeente verplicht de inwoner hiervan op de hoogte te stellen.
- Bieden van ondersteuning bij dienstverlening aan digitaal minder vaardige inwoners.

De wetgeving WMEBV en de handreiking op hoofdlijnen geanalyseerd en verwerkt in een praktisch overzicht. De drie kolommen geven wat de wet vraagt, wat dat betekent voor overheden en hoe Doccle concreet kan helpen. De toelichting is opgebouwd op basis van de officiële handreiking en beschrijvingen van de **Wet modernisering elektronisch bestuurlijk verkeer (WMEBV)**.

Eisen WMEBV (kernwoorden)	Wat betekent dit concreet voor overheden?	Hoe Doccle kan ontzorgen
1. Recht op digitaal berichtenverkeer	Burgers en bedrijven krijgen het recht om formele berichten (aanvraag, bezwaar, klacht,	Doccle biedt een gereguleerd ontvangstkader dat automatisch

Eisen WMEBV (kernwoorden)	Wat betekent dit concreet voor overheden?	Hoe Doccle kan ontzorgen
	melding) elektronisch in te dienen via een door formeel digitaal document en betrouwbare manier, met bewijs van ontvangst.	
2. Aanwijzen van digitale kanalen	Organisaties moeten een overzicht van de type duidelijk kanalen en welke digitale kanalen gebruikt mogen worden en zorgen dat deze voldoen aan de wettelijke vereisten (veilig, toegankelijk, betrouwbaar).	voldoet aan wettelijke eisen. Zo hoeft de organisatie niet elk kanaal afzonderlijk te certificeren.
3. Geen onnodige belemmeringen	Digitale formulieren en kanalen mogen geen onnodige drempels bevatten (bv. onnodige gegevens, ingewikkelde authenticatie). Burger krijgt ontvangstbevestiging en afschrift van ingevulde gegevens.	Doccle verzorgt gebruiksvriendelijke interfaces en notificaties , inclusief afschriften en ontvangstbewijzen, zonder extra ontwikkelwerk.
4. Bewijslast & traceerbaarheid	Bestuursorganen moeten aantonen dat berichten correct zijn ontvangen en behandeld; burgers hebben recht op bewijs van verzending/ontvangst.	Doccle levert een audittrail en juridische bewijsstroom : tijdstempels, statusinformatie en downloadbare bewijsstukken bovenop de communicatie.
5. Notificaties & toegankelijkheid	Voor berichten in een berichtenbox gelden notificatieverplichtingen (bijv. binnen 48 uur). Communicatie moet toegankelijk zijn voor alle doelgroepen (zorgplicht).	Doccle zorgt voor notificaties via gekozen kanalen (mail, push) en ondersteunt toegankelijkheid en inclusie door multi-channel ontvangsopties.
6. Passende ondersteuning (zorgplicht)	Organisaties moeten zorg dragen dat iedereen communicatie kan benutten (duidelijke informatie, hulp waar nodig).	Doccle verhoogt vindbaarheid en transparantie door centrale toegang en helpflows — minder verwarring, minder contactdruk op de helpdesk.
7. Integrale digitale dienstverlening	Overheden moeten digitaal verkeer en processen koppelen binnen bestaande ketens en systemen, zonder losse eilandoplossingen.	Doccle functioneert als schakelplatform tussen systemen, waardoor je niet voor elk systeem een aparte oplossing hoeft te bouwen.

Kernpunt

- WMEBV is geen technische norm; het is een **bestuurlijke verplichting tot structurele digitalisering en traceerbare communicatie**. Het doel is heldere, veilige, inclusieve en aantoonbare digitale interactie met burgers en bedrijven.

Waarom dit relevant is voor jouw doelgroep

- Gemeenten, rijksoverheid en uitvoeringsorganisaties worstelen met versnipperde kanalen, compliance-eisen en bewijsvoering. WMEBV schrijft voor wat moet — Doccle helpt **hoe je dat praktisch uitvoert**, met minder risico, lagere IT-lasten en een betere burgerervaring.

9. DataWallets - DataSluizen en DataKluizen – Overeenkomsten en verschillen

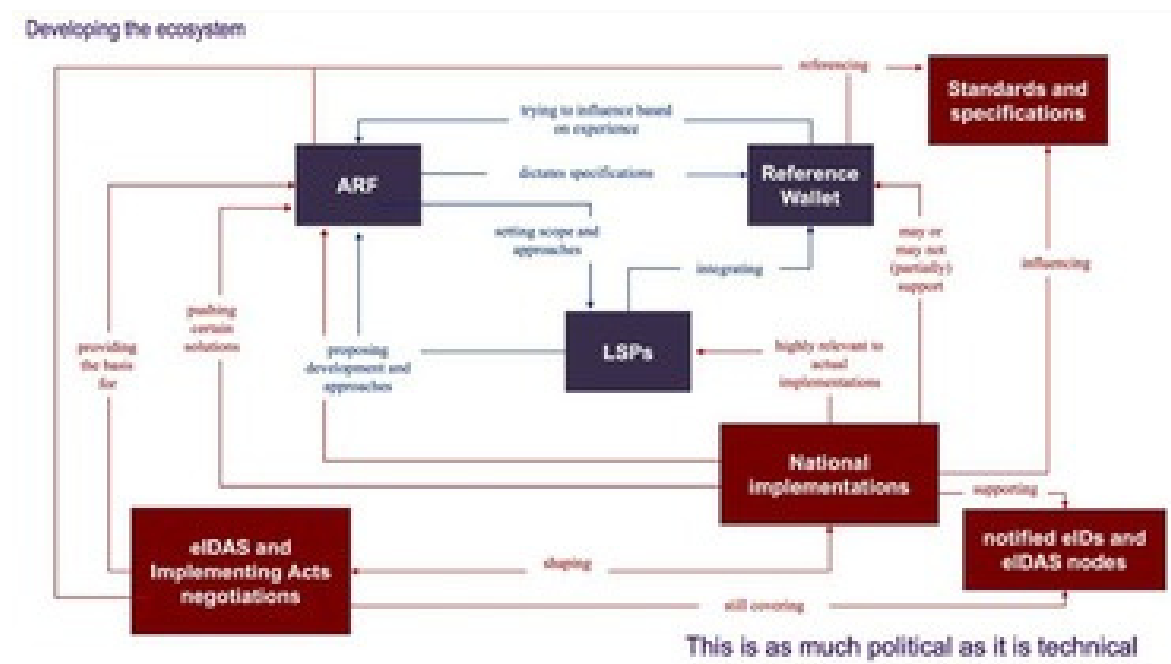
Voor organisaties komen er vele nieuwe ontwikkelingen op hen af. Zowel (EU) wetgeving en tal van nieuwe technologieën. Het blijkt lastig de mogelijkheden ervan te begrijpen en deze te beoordelen op overeenkomsten en verschillen.

Een belangrijke opkomst zijn de data wallets. Gaan deze dan alle vraagstukken oplossen?
Het antwoord is Nee, er zijn heel duidelijke verschillen en de wallets gaan zeker niet 'alles oplossen'.

Graag delen we inzichten zodat organisaties de juiste keuzes kunnen maken welke toepassing het beste past.

	Data Sluis	Data Wallet	Data Kluis – incl brondata
	v.b. VeiligOphalen, Ockto v.b. Datakeeper, Ockto		v.b. Doccle met brondata
Algemeen	Data uit de bronnen van de overheid	Data uit de bronnen van de overheid en identificatie	Ontzorgen in klantcommunicatie met optioneel data vanuit bronnen van de overheid en klant identificatie.
Waarom	Uitwisseling van betrouwbare informatie.	Veilige identificatie en efficiënte digitale processen door uitwisseling van betrouwbare informatie.	Ontzorgen van eindgebruiker, consument/ ZZP/ MKB: • Vereenvoudigen persoonlijke administratie door kijkglas te zijn Ontzorgen van organisatie: • Vereenvoudigen communicatie • Versnellen van digitale transformatie door bewezen en schaalbare technische componenten
Type informatie	Brondata attributen: • Persoons Gegevens • PSD2	Brondata attributen: • Persoons Gegevens • PSD2 • Data kaartjes (ouder dan 18 jaar)	• (Bron)Data attributen • (Bron)Documenten • Profielvragen • Life-events • Signalen
Soort informatie	• Data formele bronnen (Declared)	• Data formele bronnen (Declared)	• Data formele bronnen • Zelf toegevoegde data
Opslag	• Geen opslag, alleen doorgeven	• Telefoon	• Cloud: in jouw persoonlijke kluis / Legal Archive
EIDAS 2.0			(Q)TSP
Voldoen aan vereisten	• eID • eTimestamp • EAA	• QeID • QeTimestamp • QEAA	• (Q)eID • (Q)eTimestamp • (Q)EAA • (Q)eSignature • (Q)eSeal • (Q)eRDS • (Q)eArchiving • (Q)eLedgers

Samenhang data-wallet ontwikkeling volgens eIDAS 2.0



Dienstverleners op EU -Trust Services List

Private

en

Publieke

Bron:
BridgeHead



European Digital Identity Framework – Timeline as of March 2025

Every member state has to provide a wallet to its citizens from Dec 24, 2026 – own one or on behalf of a certified one

