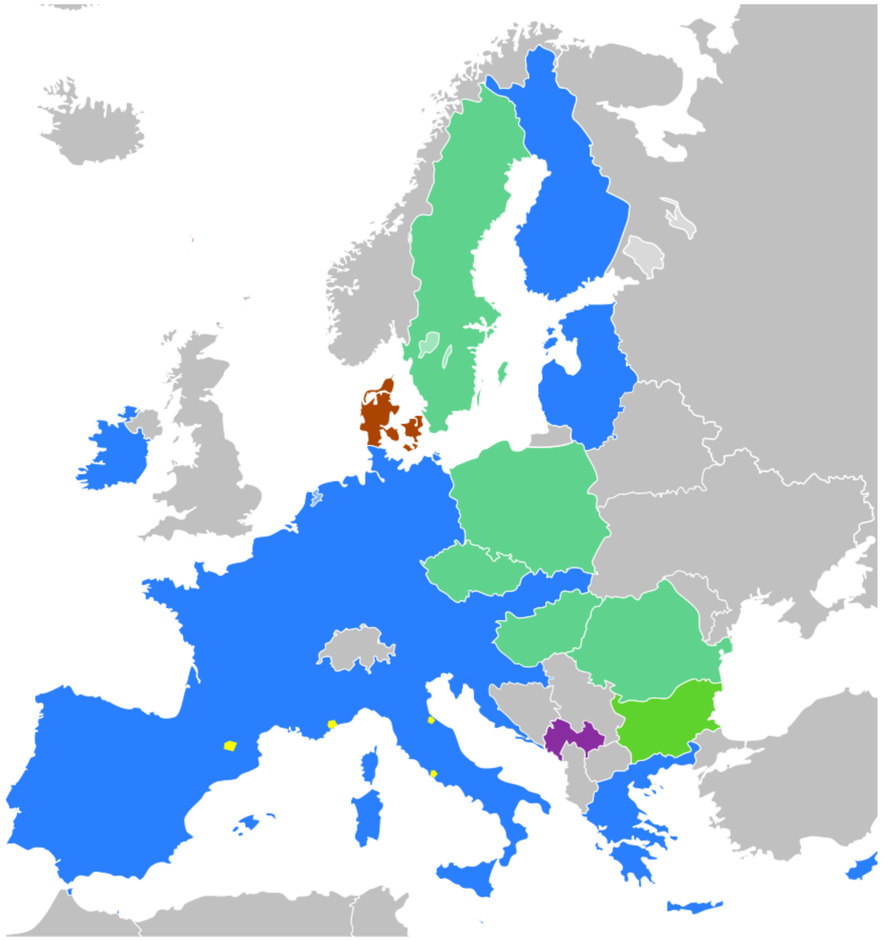
PSD3 . . .

Op weg naar beter, veiliger en efficiënter betalingsverkeer

10 oktober 2024

In Audit

Reizend door Europa in de jaren ‘90



EU-landen met de euro als munt [bewerken | brontekst be

Sinds 1 januari 2023 telt de Europese Unie 20 euro-landen.

Lidstaat	Eurozone sinds	Voormalige munteenheid
België	1 januari 2002	Belgische frank
Duitsland		Duitse mark
Portugal		Portugese escudo
Spanje		Spaanse peseta
Finland		Finse mark
Frankrijk		Franse frank
Griekenland		Griekse drachme
Ierland		Iers pond
Italië		Italiaanse lire
Luxemburg		Luxemburgse frank
Nederland		Nederlandse gulden
Oostenrijk		Oostenrijkse schilling
Slovenië	1 januari 2007	Sloveense tolar
Cyprus [1]	1 januari 2008	Cypriotisch pond
Malta		Maltese lire
Slowakije	1 januari 2009	Slowaakse kroon
Estland	1 januari 2011	Estische kroon
Letland	1 januari 2014	Letse lats
Litouwen	1 januari 2015	Litouwse litas
Kroatië	1 januari 2023	Kroatische kuna

InAudit

Veelheid aan valuta

Traveler cheques

Credit cards

InAudit

InAudit

Ontwikkeling van het Europese betalingsverkeer

- Sinds 2002 géén valutaverschillen meer binnen de Eurozone
- Ontstaan in 2014 van de Single Euro Payments Area (“SEPA”)
- Van nationale betalingsinfrastructuur naar een Europese infrastructuur
  (o.a. invoering IBAN nummers 1 augustus 2014)
- Harmonisatie nationale wet- en regelgeving inzake betaalverkeer
  door Europese richtlijnen zoals PSD2 (2015), EMD2 (2009), AMLD6 (2021) etc.

InAudit

Op weg naar veiliger, sneller en goedkoper betalingsverkeer

☑ • PSD1 - Richtlijn 2007/64/EG
- vastgesteld 13 november 2007
- in werking 1 november 2009

☑ • PSD2 - Richtlijn (EU) 2015/2366
- vastgesteld 25 november 2015
- in werking 13 januari 2018

PSD3 - Richtlijn (EU) 2024/ ?
- Status:
  - vastgesteld door de Europese Commissie (juni 2023)
  - nog goed te keuren door de Europese Raad en het Europees Parlement

InAudit

PSD1

- De PSD1 (Payment Services Directive) 2007/64/EC, werd gepubliceerd in 2007.
- De doelstelling was harmonisatie te realiseren in de Europese infrastructuur voor betalingen:
  - Gemeenschappelijke markt met gemeenschappelijke definities
  - Eenduidige en vergelijkbare regels in heel Europa
  - Realiseren van een moderne, efficiente en concurrerende markt voor betaaldiensten
  - Vergelijkbaar vergunningstelsel in heel de Europese Unie (met Europees paspoort)
  - Consumentenbescherming (transparantie, rechten)
  - Snelle verwerking overmakingen (binnen een dag)

Waar waren we in 2012 ?

InAudit

Maar de ontwikkelingen gingen snel

- In 2007 werd de eerste iPhone pas geïntroduceerd
- Digital wallets (zoals Apple Pay, Google Pay en Samsung Pay) kwamen tussen 2011 en 2015
- De NFC-techniek kwam tot ontwikkeling (basis voor contactloos betalen)

- PSD1 voorzag niet in betalen via een app op je smartphone,
- noch in nieuwe technieken die het betaalverkeer veiliger konden maken,
  zoals de EMV-chip, tokenization, two-factor authentication etc.
- Ten tijde van PSD1 was de SEPA er nog niet, pas in 2014

- Fintech bedrijven kwamen op, bijvoorbeeld Adyen (2006) en BUX (2014), Mollie (2004), Buckaroo (2005) en meer.
- Ook werd iDeal al in 2005 door de Nederlandse banken ontwikkeld voor gestandaardiseerde online betalingen

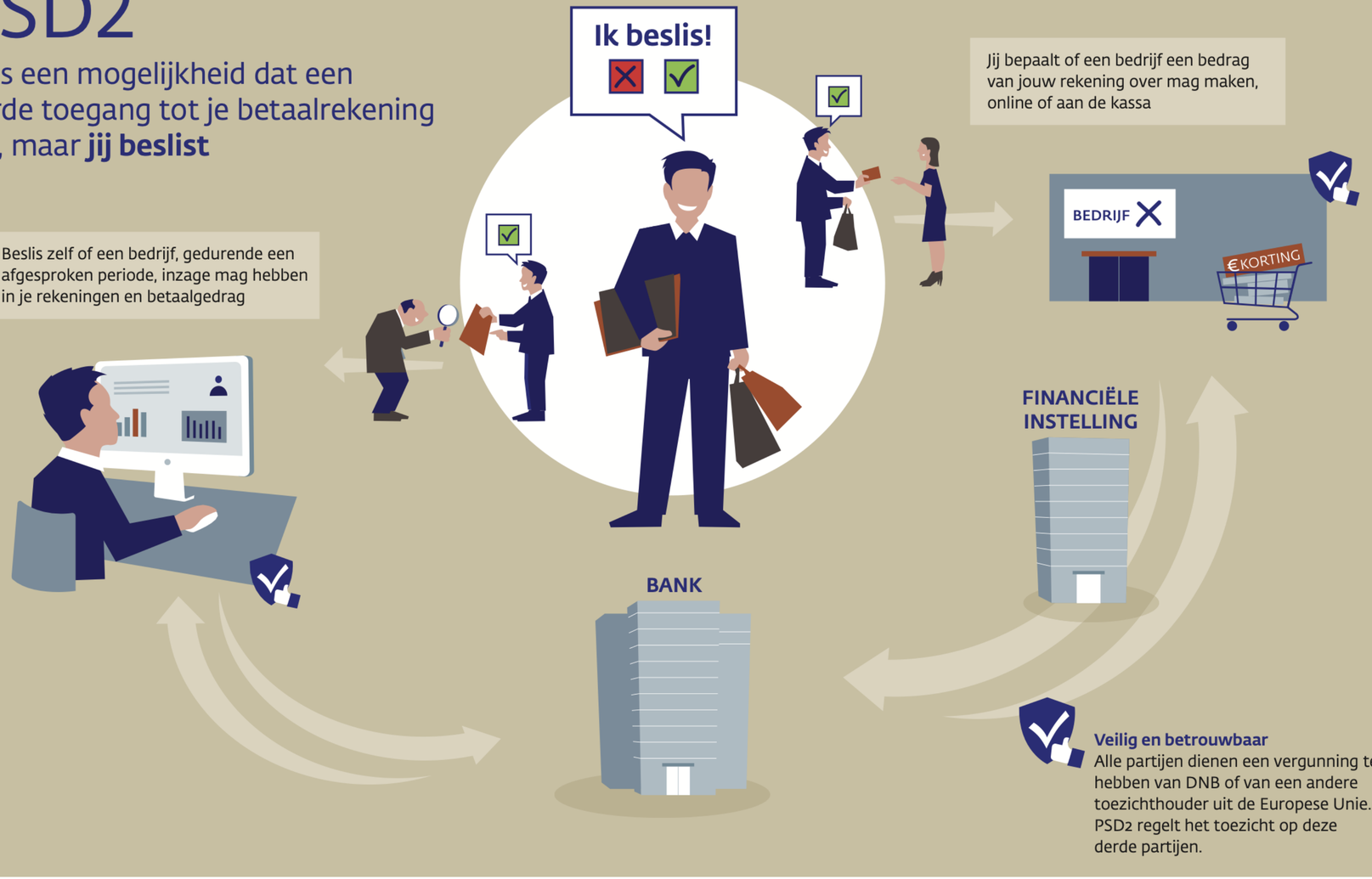
PSD2

- De PSD2 (Payment Services Directive) (EU) 2015/2366, werd gepubliceerd in 2015.
- De doelstelling was verdere verbetering van PSD1:
  - Introductie van “Open banking” – gebruik van ‘third-party providers’ voor betalingen *(artikel 66)* en account informatie *(artikel 67)*
  - Strong Customer Authentication (“SCA”) *(artikel 97 en 98)*
    - Twee van de drie: (1) iets dat je bent, (2) iets dat je hebt, (3) iets dat je weet
  - Bredere scope van instellingen die onder de richtlijn vallen *(artikel 2, overweging 6)*
  - Betere consumentenbescherming:
    - Bewijslast bij de ‘payment service provider’ *(artikel 73)*
    - Aansprakelijkheid voor de ‘payment service provider’ *(artikel 74)*
    - Beperking van de schade tot maximaal € 50 bij verlies van een ‘betaalinstrument’ *(artikel 74)*
    - Verbod op toeslagen voor het gebruik van betaalinstrumenten *(artikel 62, lid 4)*

InAudit

PSD2

Er is een mogelijkheid dat een derde toegang tot je betaalrekening wil, maar **jij beslist**



Veilig en betrouwbaar
Alle partijen dienen een vergunning te hebben van DNB of van een andere toezichthouder uit de Europese Unie. PSD2 regelt het toezicht op deze derde partijen.

InAudit

Maar de wereld staat niet stil …

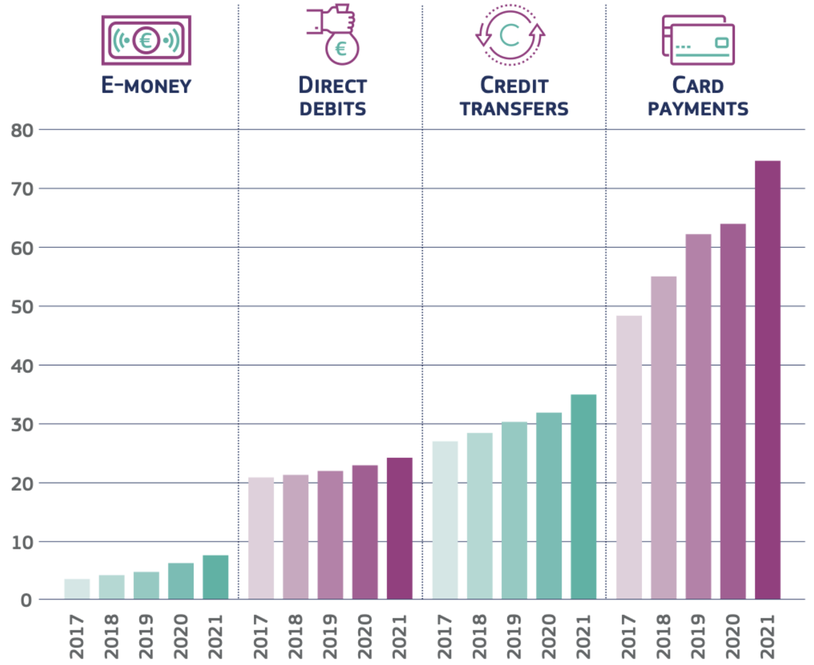
The Electronic Payments Landscape

Essential to the economy: Electronic payments in the EU: €240 trillion in 2021 (€184.2 trillion in 2017).

PSD2 (Payment Services Directive 2) is the EU legislative framework for all electronic payments, € and non-€. It contains rules on **consumer protection, security of transactions, licensing and supervision of payment service providers (PSP)**.

PSD2 needs an update, given all the **market developments** since 2015 (newer frauds, newer players/payment service providers) and **innovations** (contactless payments, QR codes, open banking).

Number of cashless payments in the EU 2017 - 2021 (in billions)



Mede door Covid een enorme sterke verschuiving naar andere vormen van betalen:

- Toenemend gebruik betaalkaarten
- Toenemend gebruik andere digitale betaalmiddelen
- Toenemend gebruik contactloos betalen
- Opkomst digitale wallets
- Nieuwe spelers en diensten
- Afnemend gebruik van contant geld

InAudit

Maar de wereld staat niet stil …

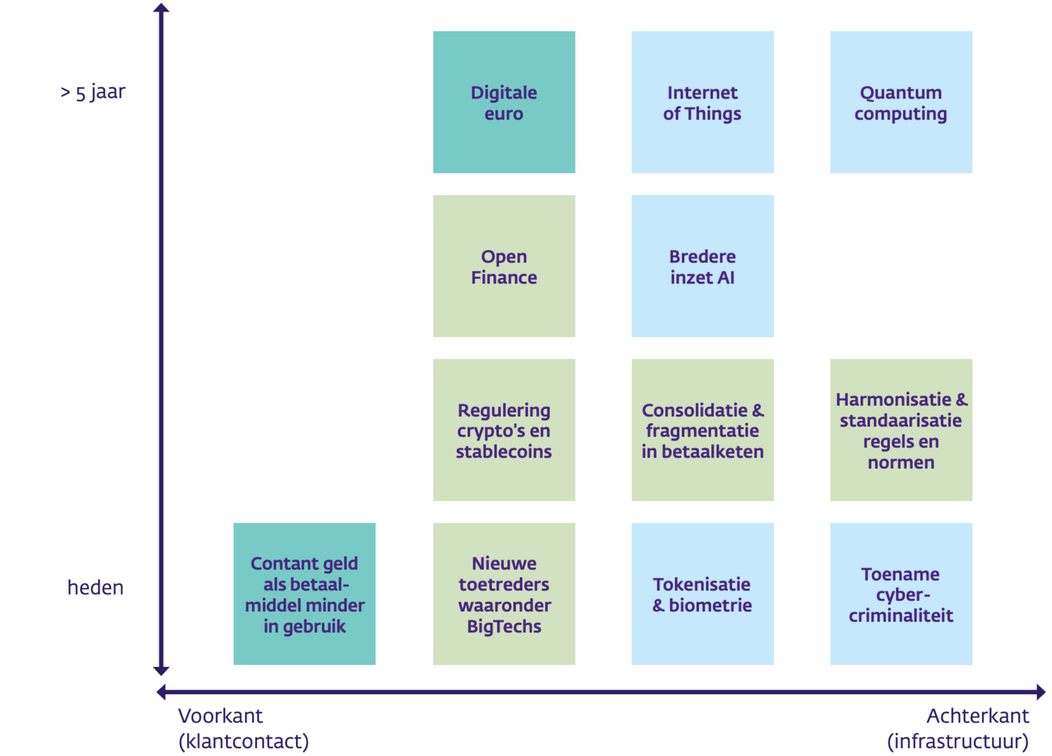
Leeswijzer

In deze publicatie komen drie speerpunten aan bod gericht op veilig, toegankelijk en efficiënt betalingsverkeer. De drie speerpunten zijn in de context geplaatst van relevante trends (zie de figuur hieronder voor een overzicht). Ook zijn de speerpunten voorzien van een visie en de inzet van DNB erbij. Sommige onderwerpen, zoals een digitale euro, raken alle speerpunten. Deze worden beschreven in Boxen.

Speerpunten

- Verankeren van robuust en veilig betalingsverkeer bij grotere digitale afhankelijkheid
- Verzekeren van toegang tot betalingsverkeer in een wereld die steeds digitaler wordt
- Versterken van betalingsverkeer in Europa en daarbuiten in een dynamisch internationaal speelveld

Belangrijke ontwikkelingen in het betalingsverkeer



Noot:
Deze figuur geeft een overzicht van belangrijke ontwikkelingen in het betalingsverkeer. Hierbij wordt aangegeven op welke termijn de ontwikkelingen ruwweg spelen, en waar in de keten zij plaatsvinden. De kleur van de blokken laat zien bij welke speerpunt de ontwikkeling nader wordt beschreven. De figuur is indicatief en slechts ter illustratie

Nederland is een aantrekkelijk land voor PSP’s

Tabel 9 Aanbieders van betaaldiensten

Aantallen (jaarultimo)

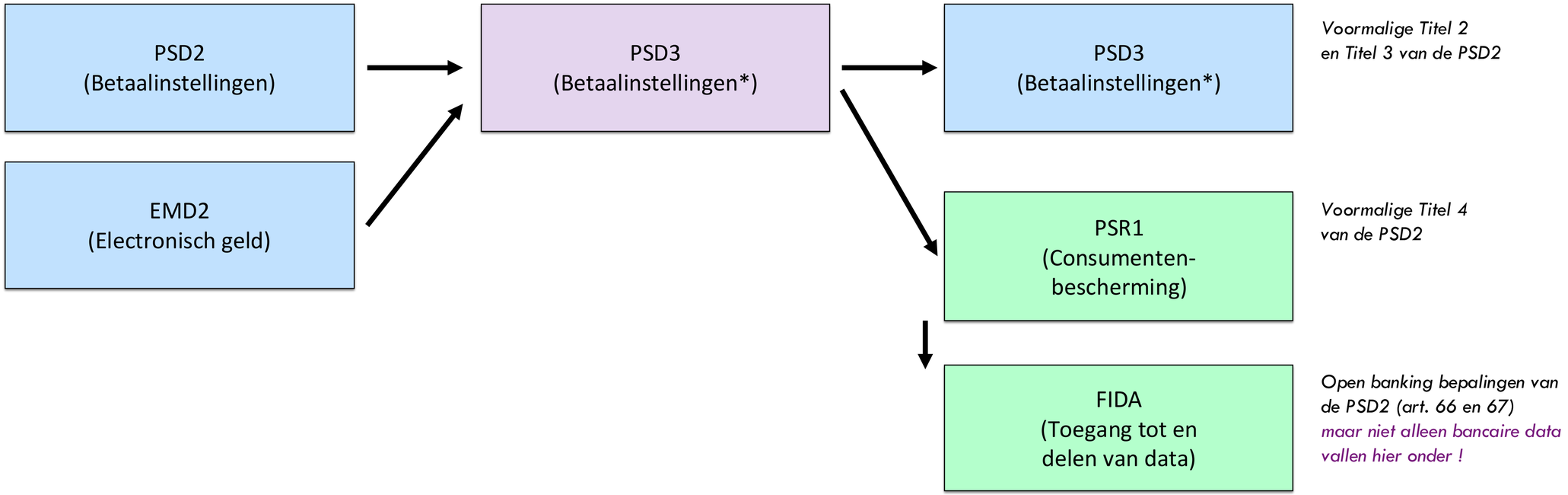
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Centrale bank											
Aantal kantoren	1	1	1	1	1	1	1	1	1	1	1
Banken											
Banken	77	74	66	52	50	45	44	41	41	42	37
Bankkantoren	2.653	2.446	2.165	1.854	1.764	1.674	1.616	1.489	1.260	942	726
Overige in Nederland geregistreerde aanbieders van betaaldiensten											
Geregistreerde wisselinstellingen	10	7	7	7	7	8	6	7	9	9	8
Elektronischgeldinstellingen[1]	2	2	2	2	2	1	1	1	5	8	10
Betaalinstellingen[1,2]	23	31	37	36	38	38	38	38	53	64	65

Bronnen: DNB en banken.

1 Genoemde aantallen zijn excusief betaal- en elektronischgeldinstellingen die een vergunning bij een nationaal bevoegde autoriteit in een andere EER-lidstaat aanhouden en geautoriseerd zijn om hun betaaldiensten (ook) in Nederland aan te bieden via het “Europees paspoort”.

2 Dankzij de invoering van PSD2 in 2019 is het aantal betaalinstellingen sterk toegenomen.

Van PSD2 naar PSD3 (en PSR1 en FIDA)



Voormalige Titel 2
en Titel 3 van de PSD2

Voormalige Titel 4
van de PSD2

Open banking bepalingen van
de PSD2 (art. 66 en 67)
maar niet alleen bancaire data
vallen hier onder !

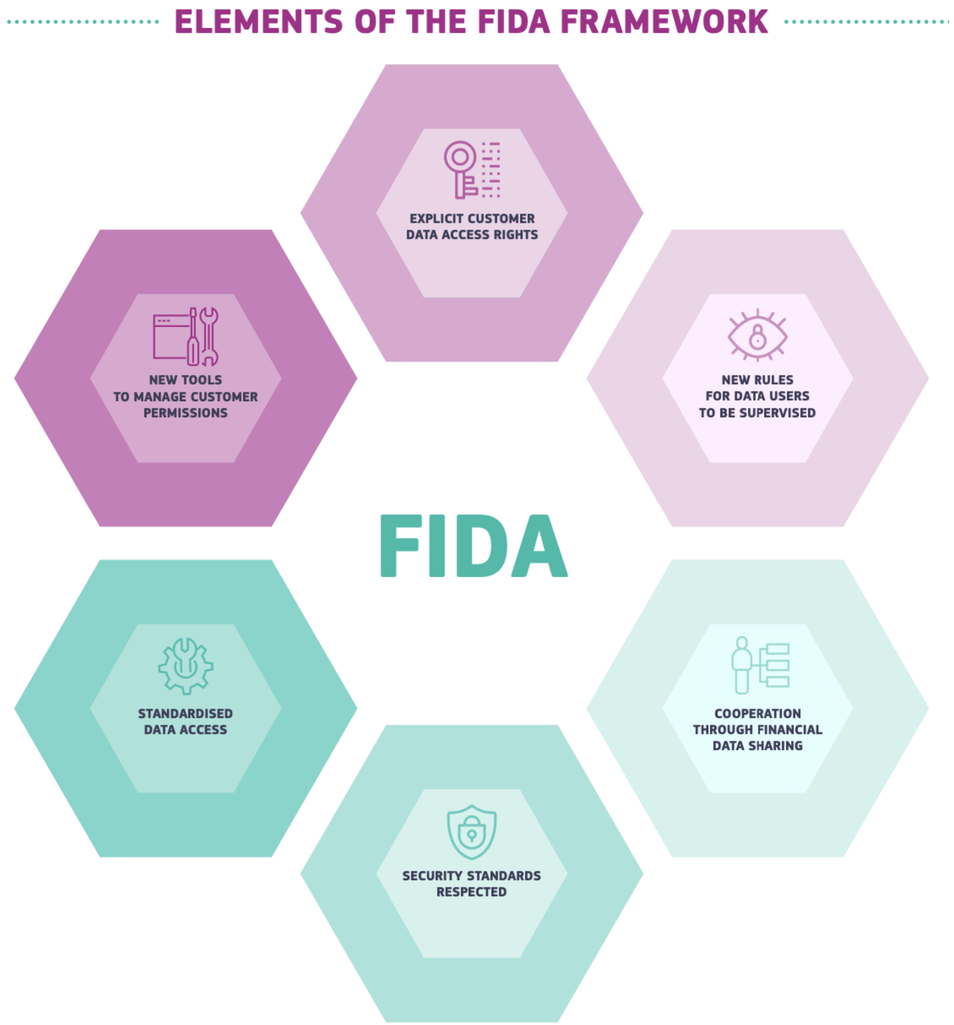
Noot:

Verschil tussen EU Directive en een EU Verordening !!!

- Verschillen in (nationale) vertaling / toepassing
- Implementatie tijd
- Rol van de EBA bij technische uitvoering

InAudit

FIDA (Financial Data Access regulation)



Scope of FIDA (producten, artikel 2, lid 1)

Deze verordening is van toepassing op de volgende categorieën cliëntgegevens betreffende:

a) *hypothecaire kredietovereenkomsten*, *leningen* en *rekeningen*, [..], met inbegrip van gegevens over het *saldo*, de *voorwaarden* en de *transacties*;

b) *spaargelden*, *beleggingen* in financiële instrumenten, verzekerings-gebaseerde *beleggingsproducten*, *cryptoactiva*, *onroerend goed* en andere *aanverwante financiële activa*, […]

c) *pensioenrechten* in het kader van *bedrijfspensioenregelingen* […];

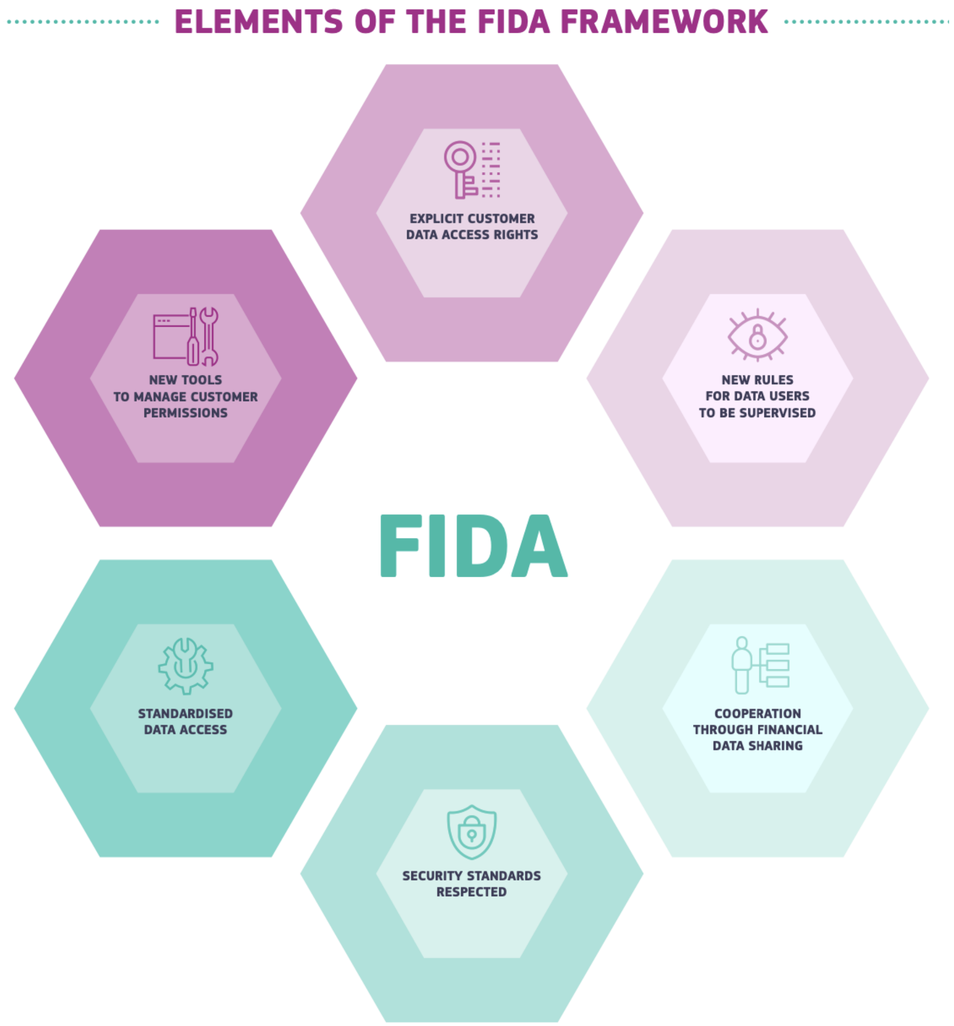
d) *pensioenrechten* in verband met de aanbieding van pan-Europese *persoonlijke pensioenproducten*, […];

e) *schadeverzekeringsproducten* […], met uitzondering van ziekte- en zorgverzekeringsproducten; met inbegrip van gegevens die zijn verzameld ten behoeve van een *verlangens-en-behoeftentest* […], en gegevens die zijn verzameld met het oog op een *adequaatheids- en geschiktheidsbeoordeling* […];

f) gegevens die deel uitmaken van een *kredietwaardigheidsbeoordeling* van een *onderneming* en die worden verzameld in het kader van een procedure voor *kredietaanvragen* of een verzoek om een *kredietrating*.

InAudit

FIDA (Financial Data Access regulation)



Scope of FIDA (entiteiten, artikel 2, lid 2)

Deze verordening is van toepassing op de volgende categorieën cliëntgegevens betreffende:

a) *kredietinstellingen*;

b) *betalingsinstellingen*, met inbegrip van rekeninginformatie-dienstaanbieders en betalingsinstellingen die zijn vrijgesteld [van PSD2];

c) *instellingen voor elektronisch geld*, met inbegrip van instellingen voor elektronisch geld die zijn vrijgesteld;

d) *beleggingsondernemingen*;

e) aanbieders van *cryptoactivadiensten*;

f) emittenten van *asset-referenced tokens*;

g) beheerders van *alternatieve beleggingsinstellingen*;

h) beheermaatschappijen van instellingen voor *collectieve belegging* in effecten;

i) *verzekerings- en herverzekeringsondernemingen*;

j) *verzekeringstussenpersonen* en nevenverzekeringstussenpersonen;

k) instellingen voor *bedrijfspensioenvoorziening*;

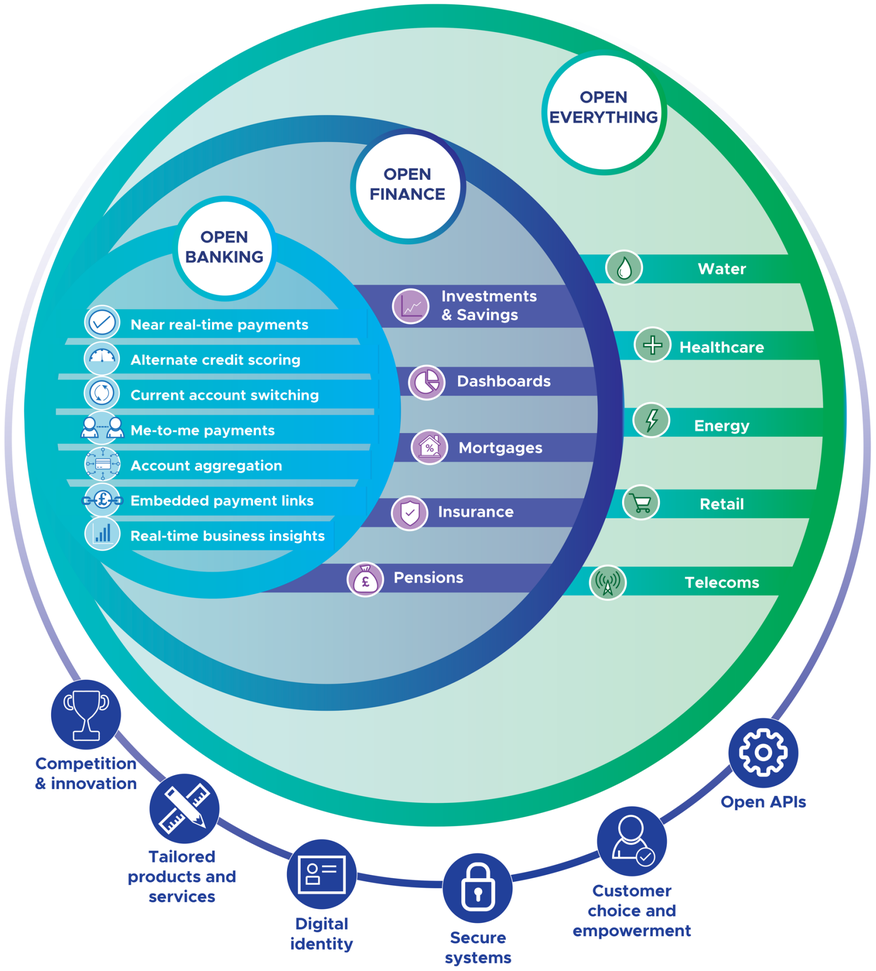
l) *ratingbureaus*;

m) aanbieders van *crowdfundingdiensten*;

n) *PEPP-aanbieders*;

o) *aanbieders van financiële-informatiediensten*.

FIDA (Financial Data Access regulation)



FIDA = Open Finance

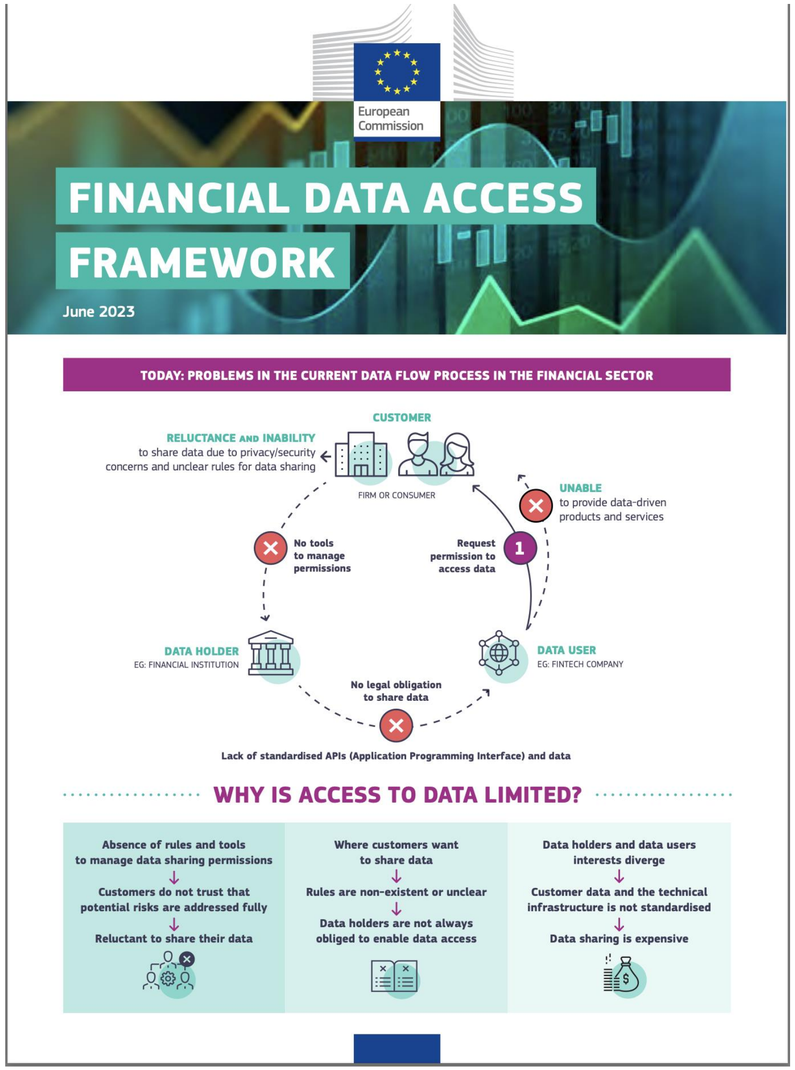
De FIDA is voorgestelde EU-regelgeving (een Verordening) die tot doel heeft het bereik van *open finance* uit te breiden door consumenten en bedrijven in staat te stellen een *breder scala* aan financiële gegevens te delen, naast betaalrekeningen.

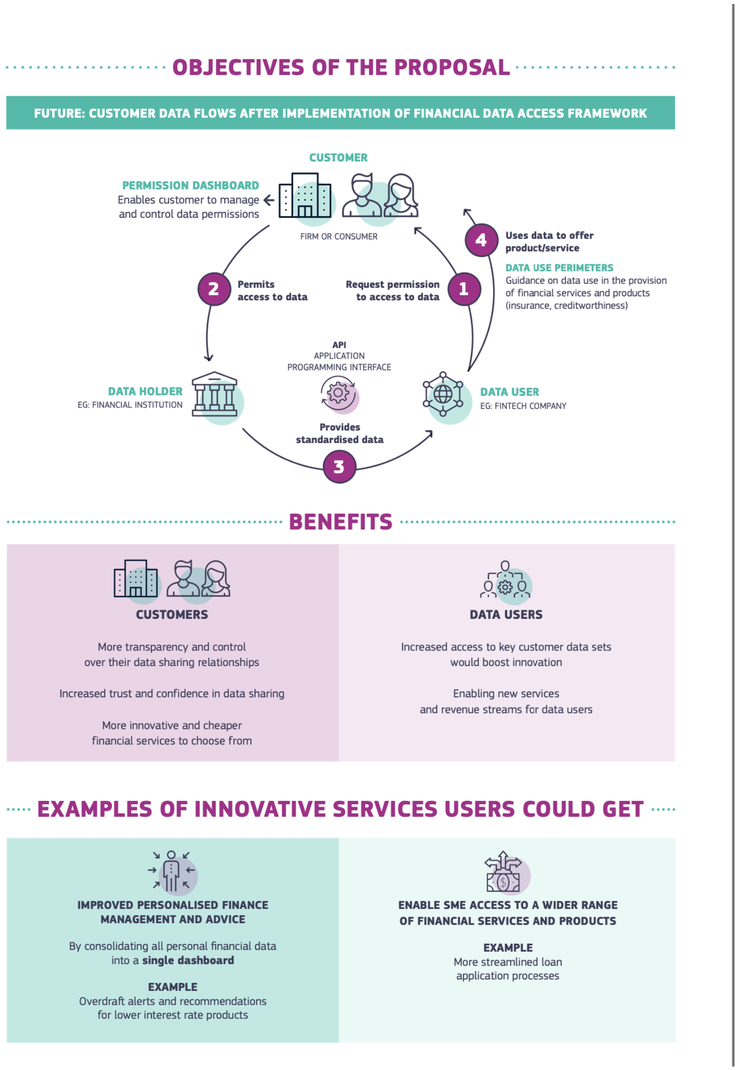
Dit omvat onder meer gegevens van hypotheken, leningen, spaarrekeningen, beleggingen, pensioenen en bepaalde verzekeringsproducten.

De verordening beoogt consumenten *meer controle* te geven over hun financiële gegevens en de ontwikkeling van *innovatieve financiële diensten* mogelijk te maken.

InAudit

FIDA (Financial Data Access regulation)





FIDA (Governance eisen)

- ## Artikel 16 - Organisatorische vereisten voor aanbieders van financiële-informatiediensten

Een aanbieder van financiële-informatiediensten voldoet aan de volgende organisatorische vereisten:

a) de aanbieder stelt *beleidslijnen en procedures* vast die toereikend zijn om de naleving van zijn verplichtingen uit hoofde van deze verordening te waarborgen, inclusief de *naleving* door zijn managers en werknemers;

b) de aanbieder neemt *redelijke maatregelen* om *de continuïteit en regelmatigheid van de uitvoering* van zijn activiteiten te waarborgen. Daartoe maakt de aanbieder van financiële-informatiediensten gebruik van *passende en evenredige systemen*, middelen en procedures om de continuïteit van zijn kritieke activiteiten te garanderen en beschikt hij over *noodplannen* en een *procedure* om de toereikendheid en efficiëntie van deze plannen regelmatig te beproeven en te herzien;

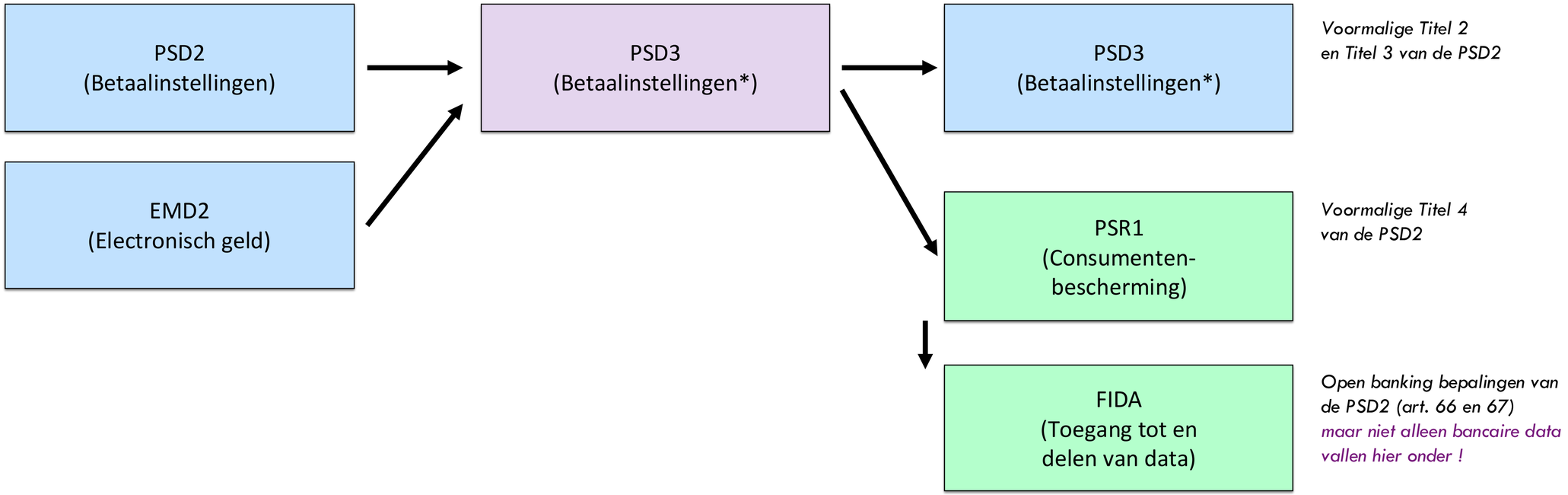
c) wanneer de aanbieder een *beroep op derden* doet voor de uitvoering van *taken die van kritiek belang zijn* voor een continue en bevredigende dienstverlening aan de cliënten en voor het verrichten van activiteiten op een continue en bevredigende basis, neemt hij redelijke maatregelen om het *operationeel risico niet onnodig te vergroten*. Uitbesteding van belangrijke operationele taken mag niet wezenlijk *afbreuk* doen aan de kwaliteit van zijn *interne controle* en aan het vermogen van de toezichthouder om te controleren of de aanbieder van financiële-informatiediensten alle verplichtingen nakomt;

d) de aanbieder beschikt over goede *governance-, administratieve en boekhoudkundige procedures*, *adequate interne controlemechanismen*, effectieve *procedures voor risicobeoordeling en -beheer*, en effectieve controle- en beveiligingsvoorzieningen voor informatieverwerkingssystemen;

e) zijn *directeuren en managers* en de personen die belast zijn met het beheer van de activiteiten van de aanbieder van financiële-informatiediensten op het gebied van gegevenstoegang zijn *betrouwbaar* en beschikken over de *nodige kennis, vaardigheden en ervaring*, zowel individueel als collectief, om hun taken uit te voeren;

f) de aanbieder zet doeltreffende en transparante procedures op voor een *snelle, eerlijke en consistente monitoring*, behandeling en follow-up van *veiligheidsincidenten* en veiligheidsgerelateerde klachten van cliënten en houdt deze procedures in stand, met inbegrip van een rapportagemechanisme dat rekening houdt met de *kennisgevingsverplichtingen* die zijn vastgelegd in hoofdstuk III van Verordening (EU) 2022/2554.

Van PSD2 naar PSD3 (en PSR1 en FIDA)



Voormalige Titel 2
en Titel 3 van de PSD2

Voormalige Titel 4
van de PSD2

Open banking bepalingen van
de PSD2 (art. 66 en 67)
maar niet alleen bancaire data
vallen hier onder !

Noot:

Verschil tussen EU Directive en een EU Verordening !!!

- Verschillen in (nationale) vertaling / toepassing
- Implementatie tijd
- Rol van de EBA bij technische uitvoering

InAudit

PSD3 en PSR – Opsplitsing van PSD2

Structuur PSD3:

- Onderwerp, scope en definities
- Betalingsinstellingen
  - Vergunning & toezicht
    - Algemene voorschriften
      - *Vergunningsvoorwaarden en procedures*
      - *Kapitaalseisen*
      - *Eigenaarschap*
      - *Boekhouding & Controle*
      - *EBA-register*
    - Dienstverlening via agenten, distributeurs etc
      - *Uitbesteding*
      - *Aanprakelijkheid*
    - Bevoegde autoriteiten en toezicht
      - *Toezicht, beroepsgeheim, rechter*
  - Vrijstellingen en kennisgevingen
    - *Facultatieve vrijstellingen*
    - *Aanbieders van rekeninginformatiediensten*
    - *Contant geld*
    - *Geldopnamediensten …*

Structuur PSR:

- Onderwerp, scope en definities
- Transparantie voorwaarden en informatievereisten
  - Algemene regels
    - *Informatieplicht, (geen) kosten, etc*
  - Eenmalige betalingstransacties
  - Raamovereenkomsten
    - *Te communiceren informatie en voorwaarden*
    - *Beëindiging*
- Rechten en plichten bij gebruik betalingsdiensten
  - Gemeenschappelijke bepalingen
  - Toegang tot betalingssystemenen rekeningen bij banken
  - Rekeninginformatiediensten en betalingsinitiatiediensten
    - Rechten van gebrukers, Interfaces
    - Rechten en plichten van aanbieders
    - Aansprakelijkheid
    - Uitvoering van betalingstransacties
    - Gegevensbescherming
    - Operationele risico's beveiligingsrisico's en authenticatie
    - Sterke cliëntauthenticatie (SCA)
    - Handhaving en klachtenprocedures

InAudit

Scope of PSD2 vs PSD3

- ## PSD 2 (artikel 2)

1. Diensten die het mogelijk maken contanten op een betaal-rekening te storten (alsmede beheer-verrichtingen)
2. Diensten die het mogelijk maken contanten van een betaal-rekening op te nemen
3. Uitvoering van betalingstransacties, met inbegrip van over-makingen van geldmiddelen […] ..
   a) Automatische afschrijvingen
   b) Transacties met behulp van een betaalkaart
   c) Doorlopende betalingsopdrachten
4. Uitvoering van betalingstransacties waarbij geldmiddelen zijn gedekt door een kredietlijn […]
5. Uitgifte van betaalinstrumenten.
6. Geldtransfers.
7. Betalingsinitiatiediensten.
8. Rekeninginformatiediensten.

- ## PSD 3 (Bijlage 1 – Betalingsdiensten)

1. Diensten die het mogelijk maken contanten op een betaal-rekening te storten en/of van een betaalrekening op te nemen.
2. Uitvoering van betalingstransacties, met inbegrip van over-makingen van geldmiddelen van en naar een betaalrekening […]
3. Uitgifte van betaalinstrumenten.
4. Acceptatie van betalingstransacties.
5. Geldtransfers.
6. Betalingsinitiatiediensten.
7. Rekeninginformatiediensten.

- ## PSD 3 (Bijlage 2 – Electronisch geld diensten)

- Uitgifte van elektronisch geld, aanhouden van betaalrekeningen waar eenheden van elektronisch geld worden opgeslagen en de overmaking van eenheden van elektronisch geld.

InAudit

SCA (Strong Customer Authentication) in PSD2 vs PSD3

PSD2 – artikel 97 – Authenticatie

Sterke cliëntauthenticatie is verplicht zodra een klant:

1. Online de betaalrekening wil bekijken
2. Een electronische betalingstransactie initieert
3. Elke actie met een risico van fraude of misbruik

Nadere details zijn uitgewerkt in een RTS
(regulatory technical standard bij de richtlijn)

lets dat je weet

lets dat je hebt

lets dat je bent

PSR – artikel 85 – Sterke cliëntauthenticatie

Sterke cliëntauthenticatie is verplicht zodra een klant:

1. Online de betaalrekening wil bekijken
2. Zich toegang verschaft tot informatie over een betaalrekening
3. Een betalingsopdracht plaats voor een electronische betalingstransactie
4. Elke actie met een risico van fraude of misbruik

Nadere details zijn uitgewerkt in een RTS
(regulatory technical standard bij de richtlijn)

PSR – artikel 3 – lid 35 – definitie 'Sterke cliëntauthenticatie'

"authenticatie die gebaseerd is op de gebruikmaking van twee of meer factoren die worden aangemerkt als kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker heeft) en inherente eigenschap (iets wat de gebruiker is) en die onderling onafhankelijk zijn, in die zin dat compromittering van één ervan geen afbreuk doet aan de betrouwbaarheid van de andere en die zodanig is opgezet dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd"

PSR – artikel 85 – lid 12 *('twee van hetzelfde')*

"De twee of meer elementen als bedoeld in artikel 3, punt 35, waarop sterke cliëntauthenticatie wordt gebaseerd, hoeven niet noodzakelijkerwijs tot verschillende categorieën te behoren, mits hun onafhankelijkheid ten volle wordt gewaarborgd."

InAudit

Voorwaarden voor vergunning *(artikel 3 en 13)*

- Op hoofdlijnen blijven de voorwaarden gelijk aan PSD2,
  met dien verstande dat …

- *Een 'afwikkelingsplan' moet worden bijgevoegd (in geval van faillissement)*
- *Bepaalde kapitaalsvereisten zijn geïndexeerd*
- *Methodes om het eigen vermogen te bepalen (artikel 7 en 8) zijn bijgewerkt*
- *Compliance met de DORA-regelgeving moet worden meegenomen*
- *DORA ICT Incidenten rapportage moet zijn ingericht*
- *Overgangsbepalingen: bestaande vergunningen lopen nog 24 maanden door,*
  maar uiterlijk binnen 18 maanden moet een nieuwe PSD3 vergunning worden 'aangevraagd'
  (ofwel: vrijstelling kan worden verleend indien de instelling aantoont compliant te zijn)

Tegengaan van misbruik en fraude (1/2)

- Artikel 50 PSR – verificatie naam en ‘unieke identificator’
  - Kostenloos, op verzoek van betalingsdienstaanbieder

- Artikel 82 PSR – melding van fraude
  - Ten minste jaarlijkse rapportage van statistische gegevens over fraude (EBA/ECB RTS-normen)

- Artikel 83 PSR – transactiemonitoringsmechanismen
  - Gebaseerd op de analyse van de betalingstransacties
  - ‘informatie over de …gebruiker met inbegrip van de omgevings- en gedragskenmerken die typisch zijn voor de gebruiker bij normaal gebruik van de persoonlijke beveiligingsgegevens’;
  - Historie betalingstransacties, transactie-informatie zelf (bedrag en identificatie begunstigde), sessiegegevens met inbegrip van IP-adresbereik
  - Rekening houdend met risicofactoren, zoals gestolen authenticatie-elementen, bedrag, fraudescenario’s, kenmerken van malwarebesmetting, abnormaal gebruik van toegangsapparatuur of software

Tegengaan van misbruik en fraude (2/2)

- Artikel 83 PSR, lid 3 – Uitwisseling unieke identificator bij voldoelde bwijs van fraude
  - Er wordt aangenomen dat er voldoende bewijs is voor het uitwisselen van unieke identificatoren wanneer ten minste twee verschillende betalingsdienstgebruikers die cliënten van dezelfde betalingsdienstaanbieder zijn, hebben meegedeeld dat een unieke identificator van een begunstigde is gebruikt om een frauduleuze overmaking te verrichten

- Artikel 84 PSR – Informatie over risico's en trends op het gebied van betalingsfraude
  - "PSP's waarschuwen hun cliënten via alle passende middelen en media"
  - Ten minste éénmaal per jaar opleidingsprogramma voor medewerkers
  - EBA Guidelines met betrekking tot dit programma

Governance
Risicobeheersing
Interne controle mechanismen

In Audit
Audit Services

FIDA (Governance eisen)

- ## Artikel 16 - Organisatorische vereisten voor aanbieders van financiële-informatiediensten

Een aanbieder van financiële-informatiediensten voldoet aan de volgende organisatorische vereisten:

a) de aanbieder stelt *beleidslijnen en procedures* vast die toereikend zijn om de naleving van zijn verplichtingen uit hoofde van deze verordening te waarborgen, inclusief de *naleving* door zijn managers en werknemers;

b) de aanbieder neemt *redelijke maatregelen* om *de continuïteit en regelmatigheid van de uitvoering* van zijn activiteiten te waarborgen. Daartoe maakt de aanbieder van financiële-informatiediensten gebruik van *passende en evenredige systemen*, middelen en procedures om de continuïteit van zijn kritieke activiteiten te garanderen en beschikt hij over *noodplannen* en een *procedure* om de toereikendheid en efficiëntie van deze plannen regelmatig te beproeven en te herzien;

c) wanneer de aanbieder een *beroep op derden* doet voor de uitvoering van *taken die van kritiek belang zijn* voor een continue en bevredigende dienstverlening aan de cliënten en voor het verrichten van activiteiten op een continue en bevredigende basis, neemt hij redelijke maatregelen om het *operationeel risico niet onnodig te vergroten*. Uitbesteding van belangrijke operationele taken mag niet wezenlijk *afbreuk* doen aan de kwaliteit van zijn *interne controle* en aan het vermogen van de toezichthouder om te controleren of de aanbieder van financiële-informatiediensten alle verplichtingen nakomt;

d) de aanbieder beschikt over goede *governance-, administratieve en boekhoudkundige procedures*, *adequate interne controlemechanismen*, effectieve *procedures voor risicobeoordeling en -beheer*, en effectieve controle- en beveiligingsvoorzieningen voor informatieverwerkingssystemen;

e) zijn *directeuren en managers* en de personen die belast zijn met het beheer van de activiteiten van de aanbieder van financiële-informatiediensten op het gebied van gegevenstoegang zijn *betrouwbaar* en beschikken over de *nodige kennis, vaardigheden en ervaring*, zowel individueel als collectief, om hun taken uit te voeren;

f) de aanbieder zet doeltreffende en transparante procedures op voor een *snelle, eerlijke en consistente monitoring*, behandeling en follow-up van *veiligheidsincidenten* en veiligheidsgerelateerde klachten van cliënten en houdt deze procedures in stand, met inbegrip van een rapportagemechanisme dat rekening houdt met de *kennisgevingsverplichtingen* die zijn vastgelegd in hoofdstuk III van Verordening (EU) 2022/2554.

In Audit
Audit Services

Governance vereisten PSR

- Artikel 81 – Beheersing operationele risico's en beveiligingsrisico's
  - 'passende risicobeperkende maatregelen en controlemechanismen'
  - Geen afbreuk aan de toepassing van (Hoofdstuk II) van DORA
  - Jaarlijkse verstrekking aan toezichthouder - geactualiseerde en uitgebreide beoordeling van risico's

- Transactierisico-analyse
  - *Overweging 115:*
    De EBA moet ontwerpen van technische reguleringsnormen opstellen met regels voor transactierisicoanalyse.

- Audits (bij uitbesteding authenticatie - SCA)
  - *Artikel 87 – recht op audits van de beveiliging*

Governance vereisten PSD3

- Overweging 21
  - Betalingsinstellingen moeten de mogelijk schadelijke gevolgen van onvolkomen vormgegeven governanceregelingen voor een degelijk risicobeheer aanpakken …
  - door op alle niveaus *een gezonde risicocultuur* toe te passen.

  - Bevoegde autoriteiten moeten toezien op de toereikendheid van interne governanceregelingen.
  - Het is passend dat de EBA *richtsnoeren inzake interne governanceregelingen* vaststelt, rekening houdend met de verschillen in omvang en in bedrijfsmodel […]

- *Maar wat is een gezonde risicocultuur ?*
- *Wat zal de EBA voorstellen in haar richtsnoeren (guidelines) ?*

Governance vereisten PSD3

- Artikel 3, lid 3 - vergunningsaanvraag
  - een beschrijving van de *governanceregelingen* en *interne-controle-mechanismen* van de aanvrager, waaronder administratieve procedures en procedures voor *risicobeheersing* en boekhouding
  - waaruit blijkt dat die governanceregelingen, internecontrolemechanismen en regelingen voor het gebruik van ICT-diensten *evenredig, passend, degelijk en adequaat* zijn;

- *Maar wat is 'evenredig, passend, degelijk en adequaat' ?*

Governance vereisten PSD3

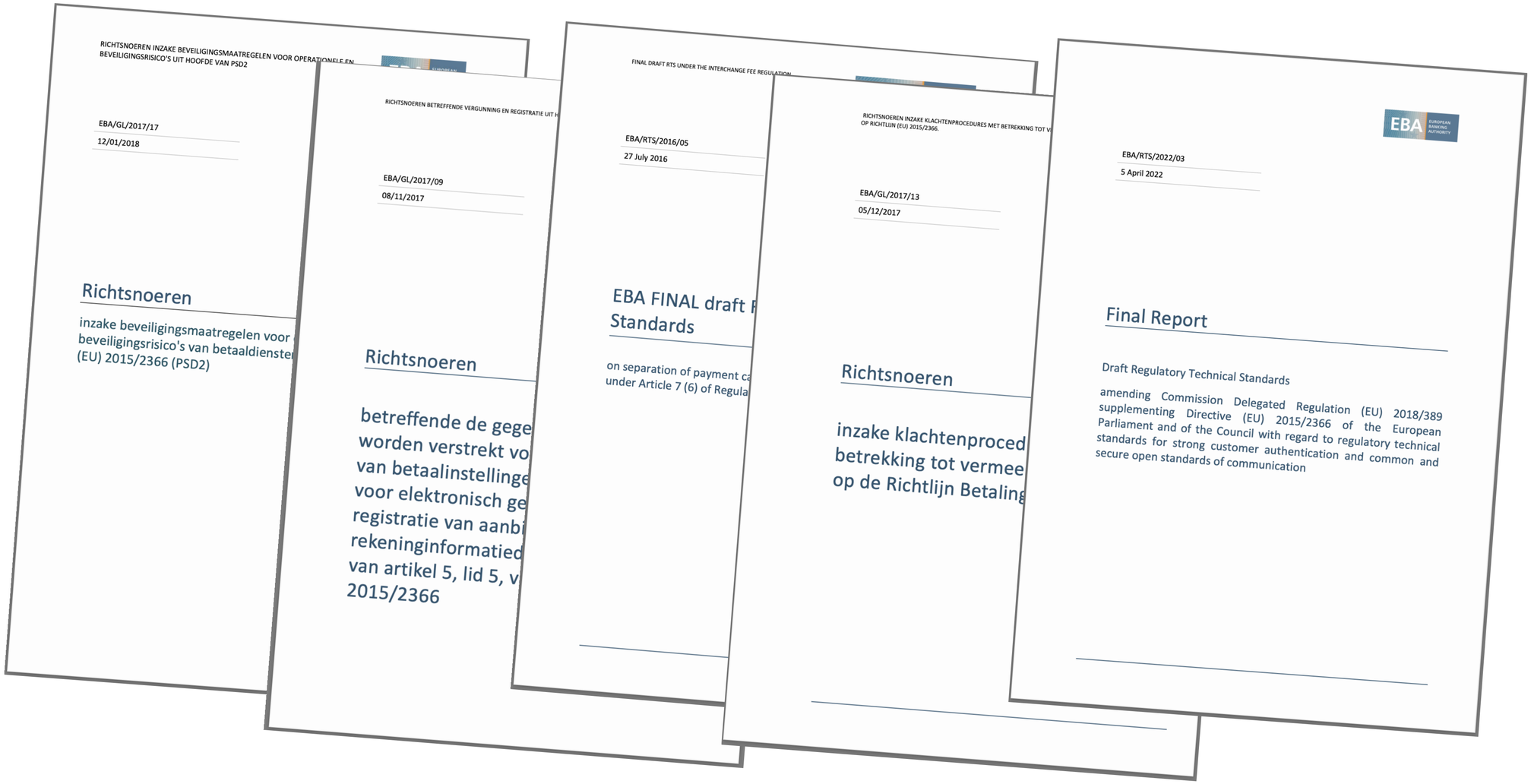
- Artikel 13, lid 1c - vergunningsverlening
  - ‘gezonde en prudente bedrijfsvoering’
  - solide governancesystemen
  - duidelijke organisatiestructuur
  - effectieve procedures
  - passende interne-controle-mechanismen

  De bedoelde governancesystemen en controlemechanismen zijn breed opgevat en staan in verhouding tot de aard, omvang en complexiteit van de betalingsdiensten of elektronischgelddiensten die de aanvragende betalingsinstelling voornemens is aan te bieden.

  - De EBA stelt richtsnoeren vast betreffende de in dit lid bedoelde systemen, processen en mechanismen.

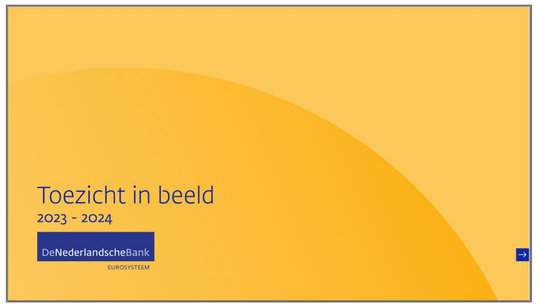
- *Maar wat zijn passende interne-controle-mechanismen ?*

Guidance vanuit de European Banking Authority (“EBA”)



Guidance vanuit DNB

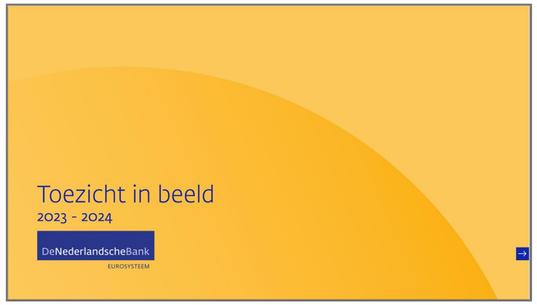
Toezicht vanuit DNB



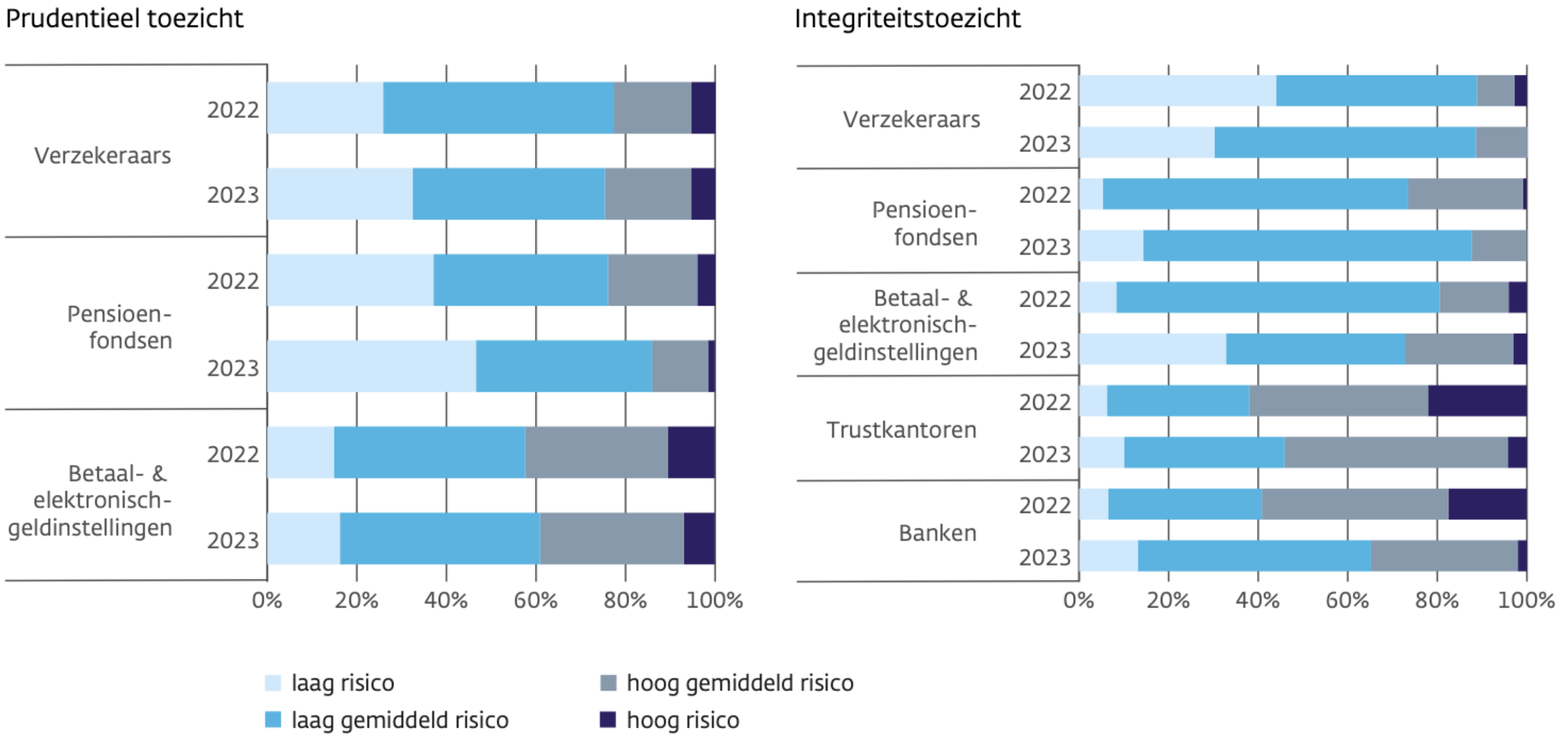
Figuur 2 Risicotaxonomie

Risico-gebieden	Prudentieel toezicht: Bedrijfsmodel en strategie	Prudentieel toezicht: GGC en risico-management	Prudentieel toezicht: Prudentiële risico's	Prudentieel toezicht: Kapitaal	Integriteits-toezicht: Integriteit
Risico-componenten	1. Levensvatbaarheid bedrijfsmodel 2. Houdbaarheid strategie	3. Interne governance 4. Gedrag & cultuur 5. Risico-management	6. Kredietrisico 7. Marktrisico 8. Renterisico 9. Operationeel risico 10. Liquiditeitsrisico 11. Verzekeringstechnisch risico	12. Kapitaalpositie	13. Witwassen 14. Terrorismefinanciering 15. Sancties 16. Corruptie 17. Maatschappelijke onbetamelijkheid

Toezicht vanuit DNB



Figuur 5 Toekenning risicocomponentscores, uitgesplitst naar sector



Peildatum: 31 oktober 2022 en 31 oktober 2023

Samenvattend

- PSD3, PSR en FIDA zijn een logische ontwikkeling in de tijd
  - Technische en marktontwikkelingen
  - Voortschrijdende inzichten nav PSD2

- PSD3, PSR en FIDA zijn ook een ingrijpende wijziging van de regelgeving
  - Verschuiving van nationaal naar Europees
  - Vast nog niet de eindfase
    - *Bijvoorbeeld: wat wordt de invloed van Artificial Intelligence en AI Agents ?*

- Ten opzichte van andere financiële richtlijnen nog weinig aandacht voor:
  - Audit, risicobeheer, 'three lines of defense'
  - Voor ICT risicobeheer wordt verwezen naar DORA
  - Nadere uitwerking van 'principle-based' begrippen als 'gezond en prudent' volgt in de EBA-guidelines

In Audit

We zien u graag op ons volgende InAudit event:

Kennisdag februari 2025

Wetgeving onder controle- van Theorie naar praktijk

Key topics:

- AI Act
- AVG, zijn we nog scherp ?
- Anti-Money Laundering

InAudit BV
Spankerenseweg 16A
6974 BC Leuvenheim
T 055 – 303 2597
W www.inaudit.nl
E info@inaudit.nl

InAudit