SIRIUS.LEGAL
BUSINESS LAW FIRM

Data Protection
Tips voor IT contracten
Data continuity

Data continuïteit is key voor een bedrijf
Je data is je kapitaal, steeds meer in digitale tijden

Dataverlies vermijden tijdens de overeenkomst

NCOI M&D Seminars

Data continuïteit is key voor een bedrijf
Je data is je kapitaal, steeds meer in digitale tijden

Dataverlies vermijden tijdens de overeenkomst

Dataverlies vermijden bij het einde van de overeenkomst

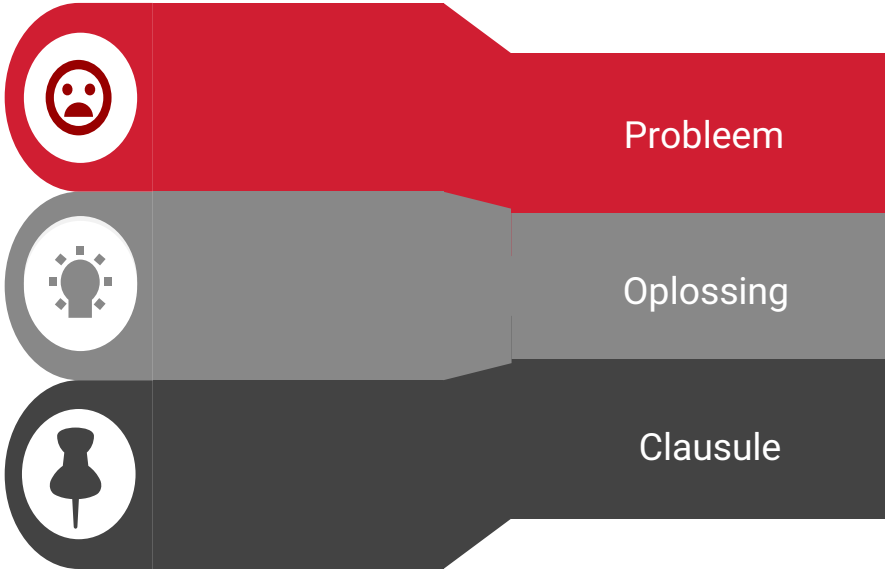
NCOI M&D Seminars

Data continuïteit is key voor een bedrijf
Je data is je kapitaal, steeds meer in digitale tijden

01 Beschikbaarheid van de dienst

02 Contractueel beschikbaarheid afdwingen

03 SLA



NCOI M&D Seminars

Aandachtspunten in een SLA

SLA is meestal in voordeel van de klant
Leverancier verbindt zich op resultaat
Commerciële druk / keuze
Voor welke processen?
Tijdskritisch / essentieel / …
Back2back met eigen leverancier

SLA is in se geen clausule
Wel bijlage bij overeenkomst
Opgelet: opportuniteit...

Kwaliteitsgarantie
Beschikbaarheid
“99,9%”
Categoriseren
Response times
Rapportage / meting
Procedures
In scope / out of scope

Dwangsom bij vertraging
Tickets / verlenging van de dienst / crediturен
Schadevergoeding (potentiële schade is soms zeer hoog

NCOI M&D Seminars

Categoriseren in SLA

1. *Prioriteitstelling*

De incidenten of vragen die niet direct door de Helpdesk van <naam opdrachtgever>

(1e lijn) kunnen worden opgelost, worden door de Helpdesk geprioriteerd en gecategoriseerd. Aan incidenten en vragen kan prioriteit 1, 2, 3, 4 of 5 worden toegekend.

Prioriteit	Prioriteitcode	Omschrijving
Hoog	1	Die incidenten waarbij de software in het geheel niet meer functioneert of waardoor de functionaliteit zodanig is afgenomen dat dit als zodanig wordt ervaren. Workaround is niet mogelijk
Hoog	2	Die incidenten waarbij de software gedeeltelijk niet meer functioneert maar waarbij het bij de overgebleven functionaliteit toch redelijk mogelijk blijft om te kunnen functioneren. Workaround is mogelijk.
Normaal	3	Problemen die zo spoedig mogelijk opgelost dienen te worden. De software werkt, echter deze problemen hebben tot gevolg dat gebruikers minder efficiënt kunnen werken.
Laag	4	Overig, onder andere vragen
	5	Requests for Change

NCOI M&D Seminars

Service Levels in SLA

Processen/ Diensten	Indicator	Omschrijving	Servicelevel per prioriteit (Streeftijden)[2]	Niveau[3]
Intake Incidenten	Bereikbaar-heid/Reactie-tijd	Het doen van een terugkoppeling op basis van een door de Helpdesk aangemeld incident met daarbij: ● een (eerste) controle op compleetheid van het aangemelde incident ● een (eerste) controle op juistheid doorverwijzing	P1: 1min/1 uur P2: 1 min/1 uur P3: 1min/8 uur P4: 1min/16 uur	90%
Terug-koppeling Incidenten	Responsetijd	Het doen van een opgave op basis van een aangemelde incident door de Helpdesk van <naam opdrachtgever> met daarbij: een korte impactanalyse met daaraan gekoppeld een oplossingsalternatief en een urenschatting voor de te nemen acties.	P1: 2 uur P2: 2 uur P3: 8 uur P4: 16 uur	90%
Oplossing Incidenten	Streeftijd Oplossing	Aandragen oplossing incident en de terugkoppeling ervan aan de Helpdesk	P1: 4 uur P2: 8 uur P3:24 uur P4:24 uur	90%

NCOI M&D Seminars

Rapportage in SLA

7. Rapportage

<naam opdrachtnemer> rapporteert aan <naam opdrachtgever> over de in deze SLA overeengekomen servicelevels.

Wekelijks wordt aangaande het proces Incident en Problem Management over de onderstaande (correctieve) rapportage items gerapporteerd.

- aantal calls, openstaand en afgehandeld;
- hoeveelheid gemelde incidenten, classificatie en oplostijden verdeeld naar categorie
- aantal escalaties, inclusief evaluatie;
- inzet van mensen en middelen;

Maandelijks wordt aangaande het proces Change Management over de onderstaande rapportage items gerapporteerd.

- uitgevoerde en doorgevoerde wijzigingen;
- status uitgevoerde (maatwerk)wijzigingen;
- status wijzigingsvoorstellen met overzicht prioriteit, status, geplande releases, voortgang etc.;

NCOI M&D Seminars

Beschikbaarheid in SLA

ARTIKEL 2 – BESCHIKBAARHEID VAN DIENST

a. DIENSTVERLENER garandeert een beschikbaarheid van minstens 99,4% per maand en 99,8% op jaarbasis. DIENSTVERLENER kan een back-up oplossing voorzien om de gewaarborgde beschikbaarheid te bereiken.

a. Het niveau van beschikbaarheid van de dienst wordt berekend op basis van het gemiddelde dat deze dienst functioneerde, conform wat overeengekomen is gedurende een bepaalde referentieperiode:

$$B = \frac{100\% * (T - \Sigma t)}{T}$$

Waar:

- B = het niveau van beschikbaarheid van de dienst.
- Σt = het totaal aantal minuten dat de dienst niet functioneerde gedurende de referentieperiode verminderd met de specifiek uitgesloten storingen (in minuten), zoals gedefinieerd in artikel 2 c.

T = het totaal aantal minuten in de specifieke referentieperiode, verminderd met de specifiek uitgesloten storingen (in minuten), zoals gedefinieerd in Artikel 2 d.

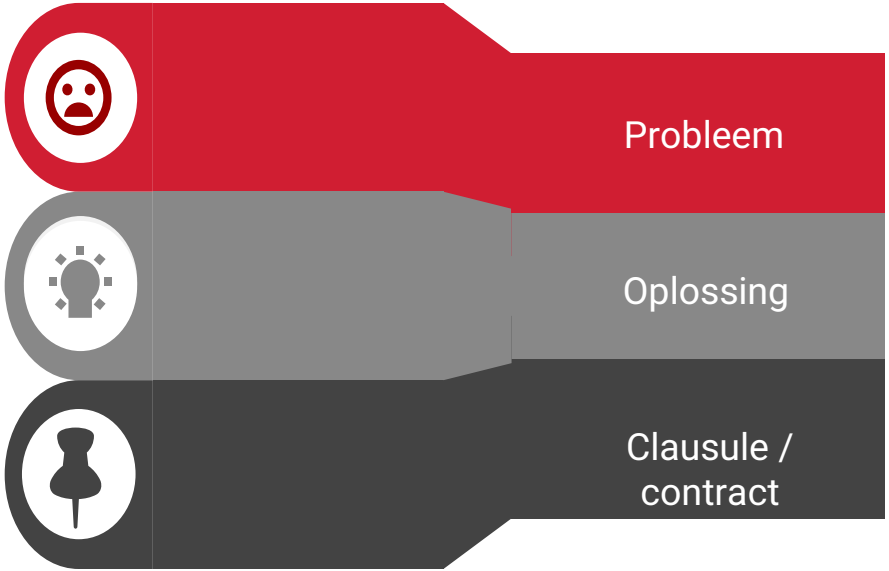
NCOI M&D Seminars

Data continuïteit is key voor een bedrijf
Je data is je kapitaal, steeds meer in digitale tijden

01 Data potentieel onbeschikbaar

02 Toegang garanderen

03 Uitsluiten ENAC SLA



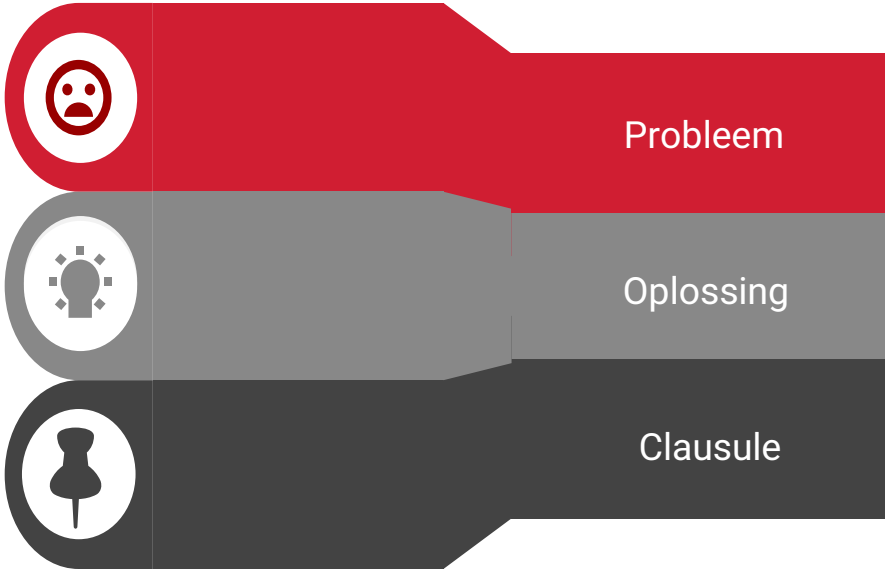
NCOI M&D Seminars

Data continuïteit is key voor een bedrijf
Je data is je kapitaal, steeds meer in digitale tijden

01 Integriteit van de data

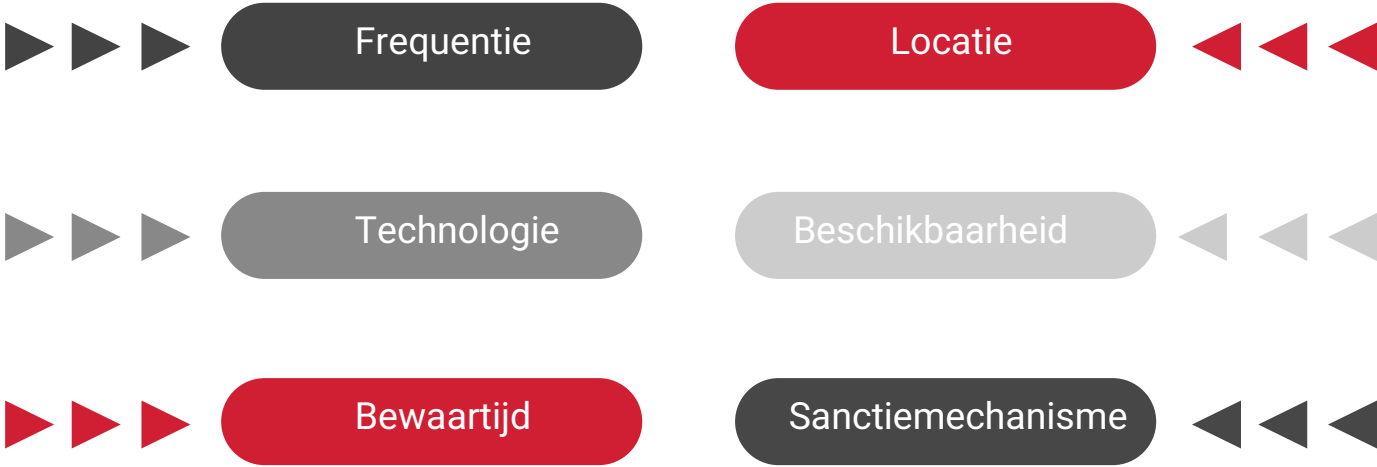
02 Veilige periodieke kopie van de data

03 Back-ups en beschikbaarheid



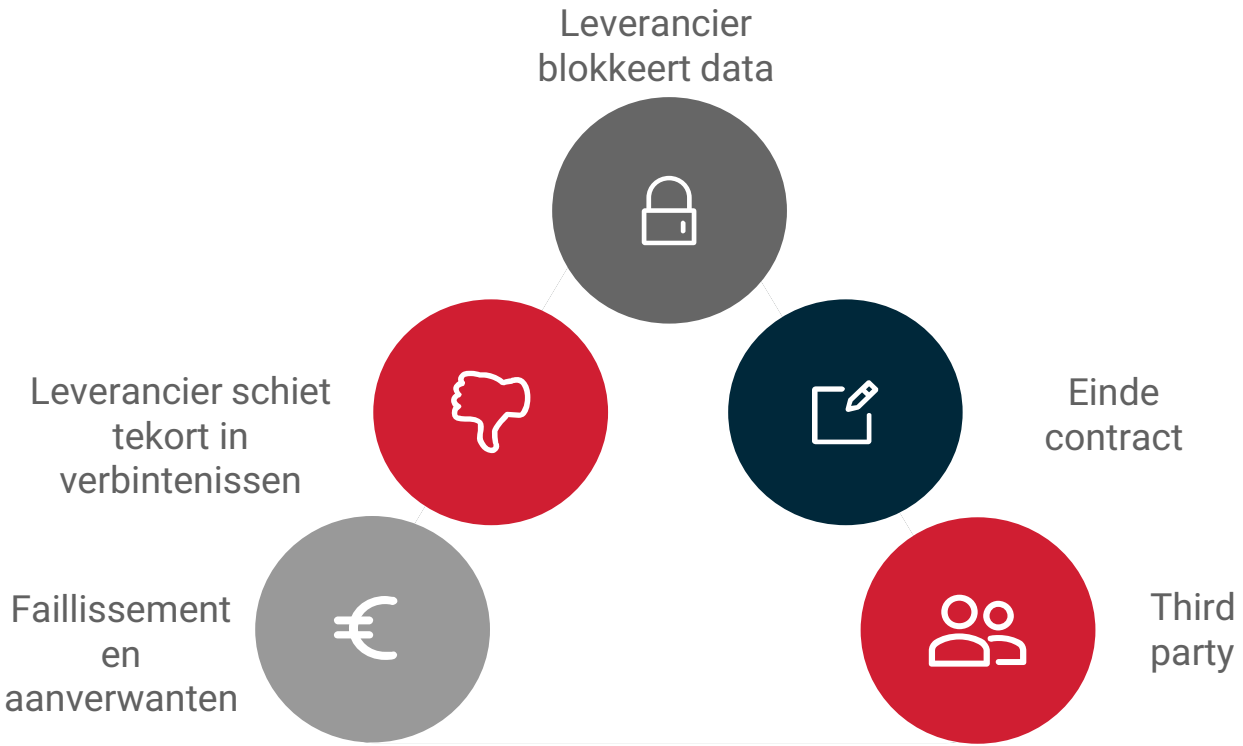
NCOI M&D Seminars

Back-up garanties in overeenkomsten



NCOI M&D Seminars

Potentiële conflictsituaties rond data



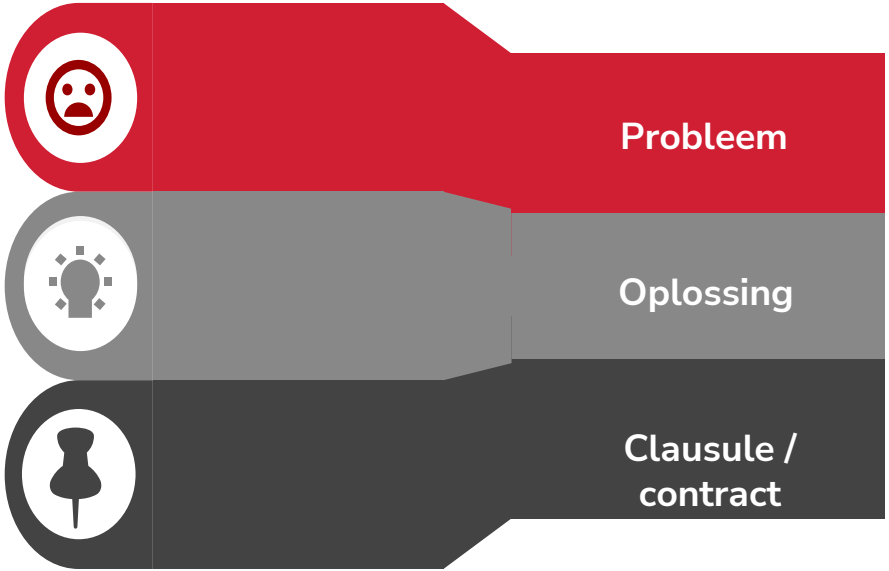
NCOI M&D Seminars

Potentiële conflictsituaties rond data

01 Data potentieel onbeschikbaar

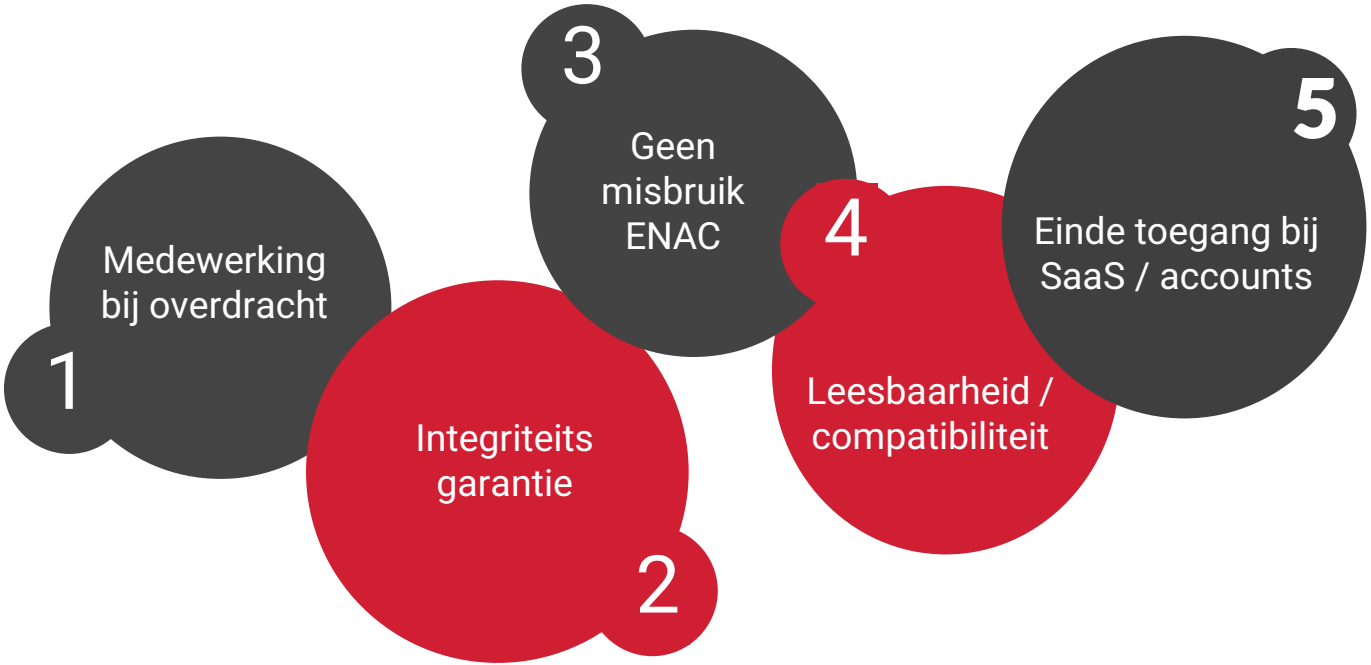
02 Toegang garanderen

03 Exitclausules Source Code Escrow



NCOI M&D Seminars

Exitclausules bij einde overeenkomst



Aandachtspunten mbt data bij einde overeenkomst

12.3 Bij het einde van de samenwerking zal steeds de continuïteit van de werking van de opdrachtgever vooropstaan zodanig dat de dienstverlener zich ertoe verbindt om alle ontwikkelde software met alle noodzakelijke documenten en informatie, paswoorden, enz… over te dragen aan de opdrachtgever, voor zover de opdrachtgever hierover niet reeds zou beschikken via de afgesproken kanalen (art. 4). Deze overdracht dient plaats te vinden uiterlijk op het tijdstip waarop de overeenkomst een einde neemt.

Op de datum van het einde van de overeenkomst zal de opdrachtgever de diensten, die werden toevertrouwd aan de dienstverlener, hernemen zonder dat deze laatste rechten mag laten gelden op de ontwikkelde software en/of de data. Inbreuk hierop geeft recht op de forfaitaire schadevergoeding, vermeld in artikel 14, onverminderd eventuele hogere werkelijk geleden schade.

Bij het einde van de samenwerkingsovereenkomst, om welke reden dan ook, zal de toegang tot de accounts en de systemen van de opdrachtgever, zoals bepaald in artikel 4, worden ontzegd.

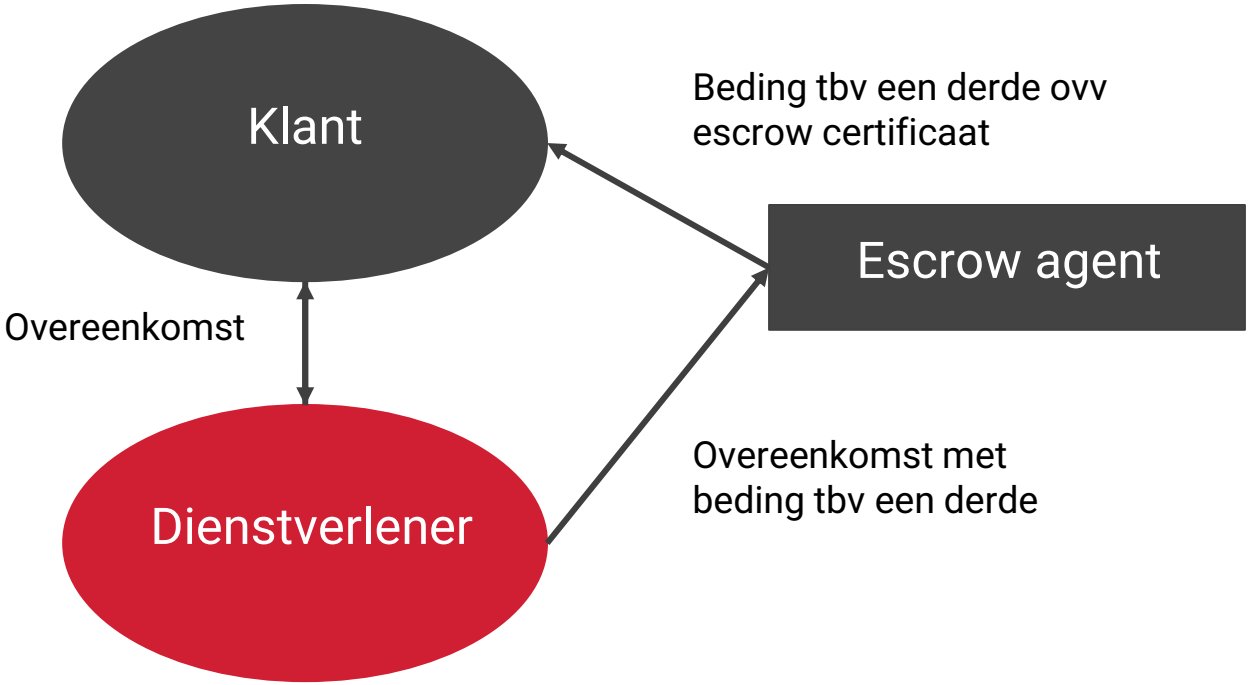
Een inbreuk op de bepalingen onder dit artikel 12.3 geeft recht op een forfaitaire schadevergoeding in het voordeel van de opdrachtgever ten bedrage van 500 € per inbreuk en per dag vertraging, onverminderd eventuele hogere werkelijke geleden schade.

Aandachtspunten mbt data bij einde overeenkomst

9.3. In case of termination Licensee is entitled to use any software already delivered by Licensor and paid by Licensee. Licensor on the other hand, shall be entitled to retain all sums heretofore paid to him. Furthermore Licensor will be equally indemnified for the software and implementation services delivered during the period of time between the date of the last issued invoice and the date of termination, and be indemnified for the services rendered subsequent to the date of termination and that arise out of such termination.

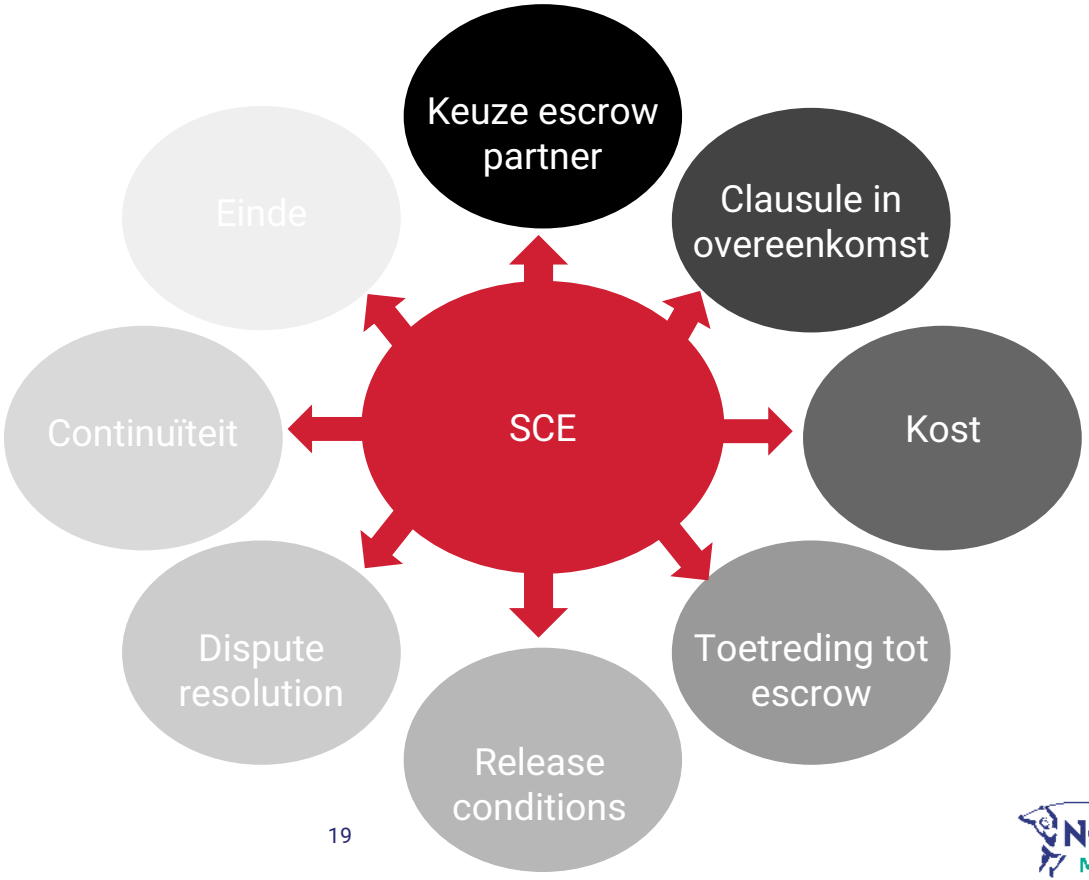
9.4. In case of termination, Licensor shall provide all necessary and reasonable assistance to Licensor in order to ensure business continuity and transfer of data to an new service provider. Licensor shall withhold from any data retention on whatever grounds, including the existence of any unpaid invoices. Any time required from Licensor during the exit or transition period shall be invoices at Licensor's standard hourly rates.

Source Code Escrow



NCOI
M&D Seminars

Source Code Escrow



NCOI M&D Seminars

Source Code Escrow

10.2. SOURCE CODE ESCROW

102.21. Upon LICENSEE's request, LICENSOR will offer adherence to its standard Source Code Escrow Agreement, which is operated by the company under Dutch law B.V. Escrow4All under standard market-based terms and conditions or through another reputable third party escrow agent of Licensor's choice. All costs for such software source code escrow service are borne by the LICENSEE.

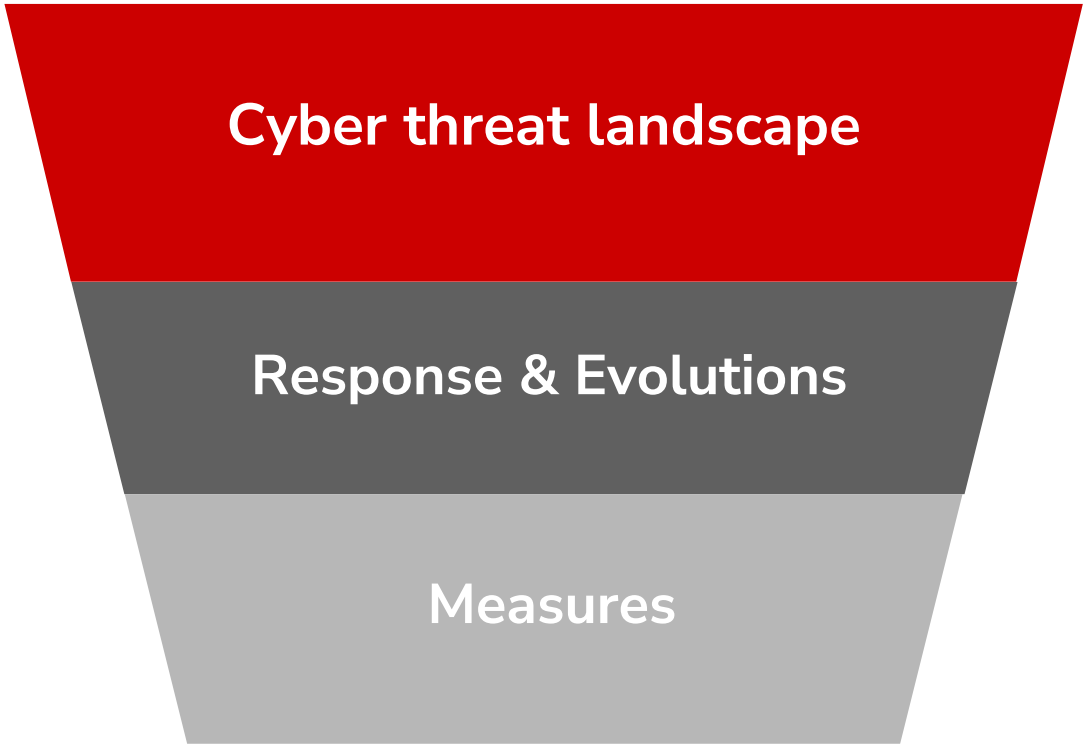
102.3. The escrow agreement shall provide for a release of the source code and associated Documentation under the events included in the escrow agreement such as: LICENSOR becomes insolvent, bankrupt or seeks protection, whether voluntary or involuntary, under any bankruptcy law. The Source Code Escrow shall in any event only provide in release of the Software in the form of a non-exclusive license limited to Maintenance of existing Software and explicitly excluding any transfer of intellectual or physical property rights to the LICENSEE.

102.4. Change of ownership in LICENSOR shall under no circumstance be a valid reason to invoke access to the Source Code Escrow by the LICENSEE. LICENSOR shall perform its best efforts to obtain continuity of the Source Code Escrow in case of change of ownership in LICENSOR.

102.5. Suspension of Licensor's services following a commercial dispute between parties or Force Majeure shall under no circumstances be a valid reason to invoke access to the Source Code Escrow by the LICENSEE.

NCOI M&D Seminars

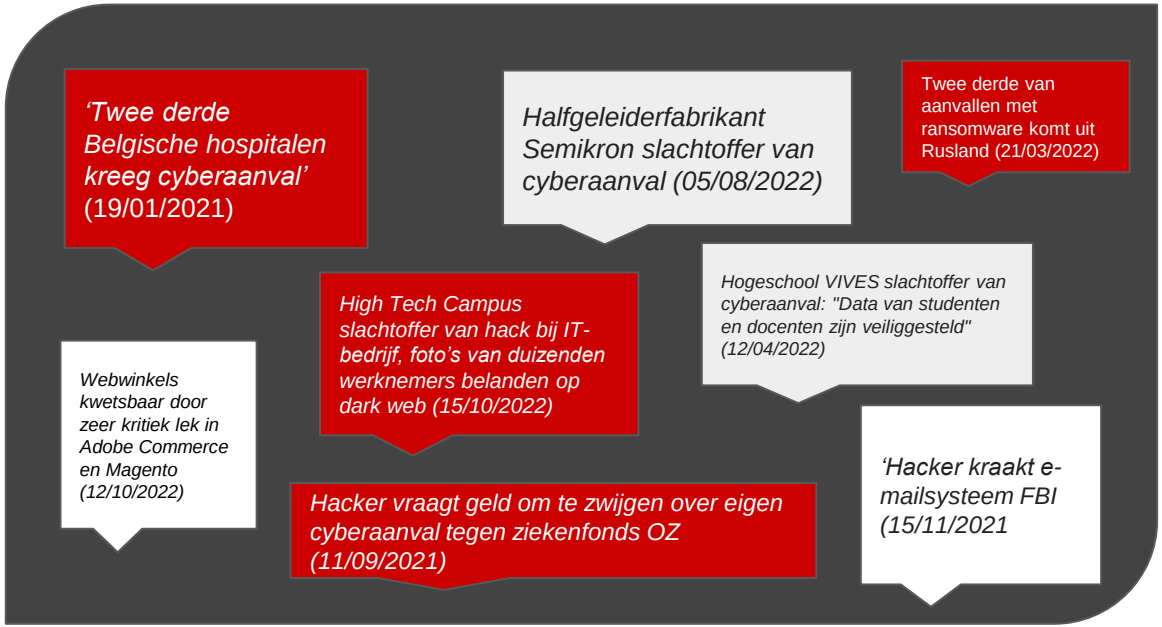
That morning in the office


Cyber threat landscape
Response & Evolutions
Measures

Cyber threat landscape

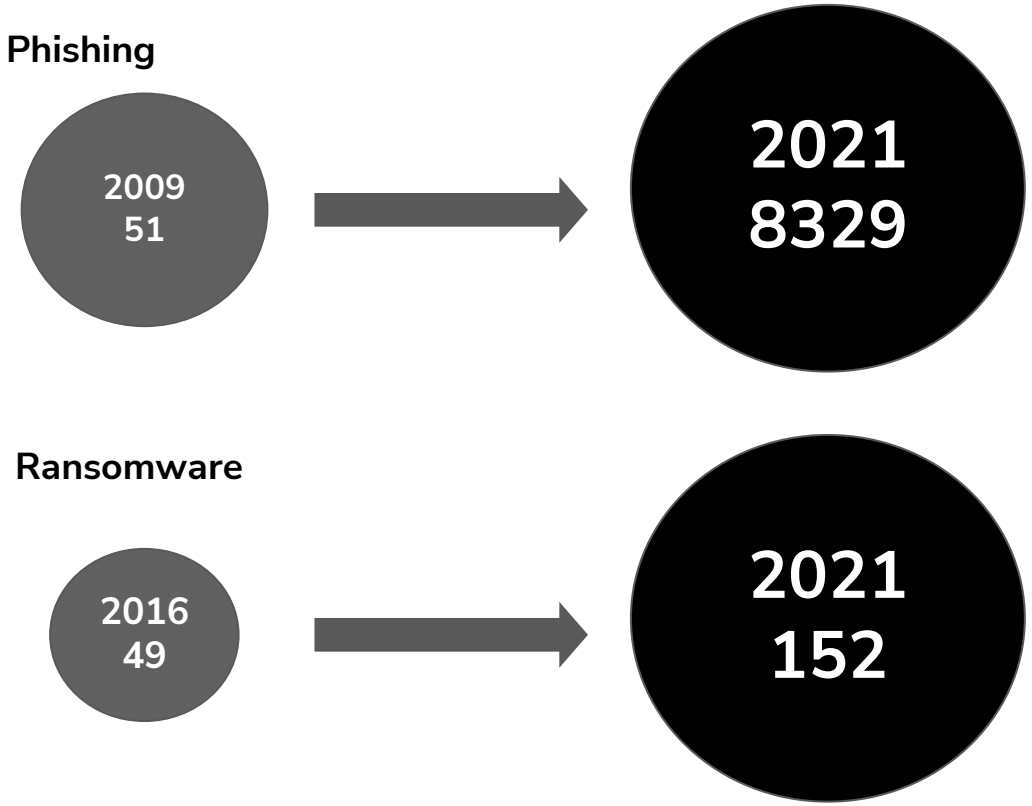
Cyber threat landscape

Berichten uit de media



Cyber threat landscape

Belgium - Police Crime Statistics 2000-2021



Cyber threat landscape

Belgium - Police Crime Statistics 2011-2021

ICT/online-crime in strikte zin

Inbreuken (exhaustief)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Informaticacriminaliteit: Informaticabedrog:	14.131	15.176	14.630	13.904	14.677	17.194	17.645	20.217	28.113	35.213	39.102
Informaticacriminaliteit: Hacking:	1.088	2.015	1.745	2.055	2.174	2.367	2.643	3.660	4.166	5.520	4.529
Informaticacriminaliteit: Valsheid in informatica:	434	472	496	647	797	764	806	1.256	1.694	3.362	3.547
Informaticacriminaliteit: Sabotage:	119	4.379	1.186	431	426	508	511	514	495	407	382
Misdr. tegen andere morele waarden en gevoelens: Schenden van communicatie door particulier:	100	108	88	85	82	67	79	75	72	67	48
Misdr. tegen gezag van de overheid: Weigering medewerking (informatica en telecom):	8	8	5	15	1	15	18	31	41	103	81
Sociaal strafwetboek: Misdr. tegen openbare trouw in sociaal strafrecht: Valsheid in informatica	5	14	19	19	22	21	25	31	46	61	51
Onwettige uitoefening van het openbaar gezag: Schenden van communicatie door ambtenaar:		1			1		2	2	6	5	9
Algemeen totaal strikt:	**15.885**	**22.173**	**18.169**	**17.156**	**18.180**	**20.936**	**21.729**	**25.786**	**34.633**	**44.738**	**47.749**

Criminele figuren (apart bekijken - niet optellen met iets anders - risico op dubbeltelling!)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Betaalkaartfraude	9.643	9.721	9.324	8.043	8.430	9.903	9.854	9.505	11.608	9.066	10.320
Phishing	91	234	341	303	220	219	474	1.316	2.462	7.525	8.329
Shouldersurfing	1.228	1.333	942	758	748	1.097	1.443	1.273	1.461	607	353
Skimming	544	569	501	432	450	475	340	263	389	297	204
Ransomware						49	239	185	178	124	152

Cyber threat landscape

Internationaal

IOCTA 2021

Threat Landscape 2021

Cyber threat landscape

Some visuals....

1. informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2. cybermap.kaspersky.com/

Cyber threat landscape

World Economic Forum

Most worrisome:
Cyberattacks & data fraud: 50,1%

Rise in priority following COVID 19:
Information security: 44,7%
Business continuity & resilience: 42,0%

Cyber resilience:
response

Legislative initiatives

1 NIS

Op wie van toepassing?

Essentieel

1. Energie
2. Transport
3. Financiën
4. Gezondheidszorg
5. Drinkwater
6. Digitale infrastructuren

Digitaal

1. Online marktplaatsen
2. Online zoekmachines
3. Clouddienstverlener

! Geen kleine of micro-onderneming =
- < 50 personen

én
- < 10 miljoen Euro (jaaromzet of balanstotaal)

Cyber resilience

1 NIS

Op wie van toepassing?

Essentieel

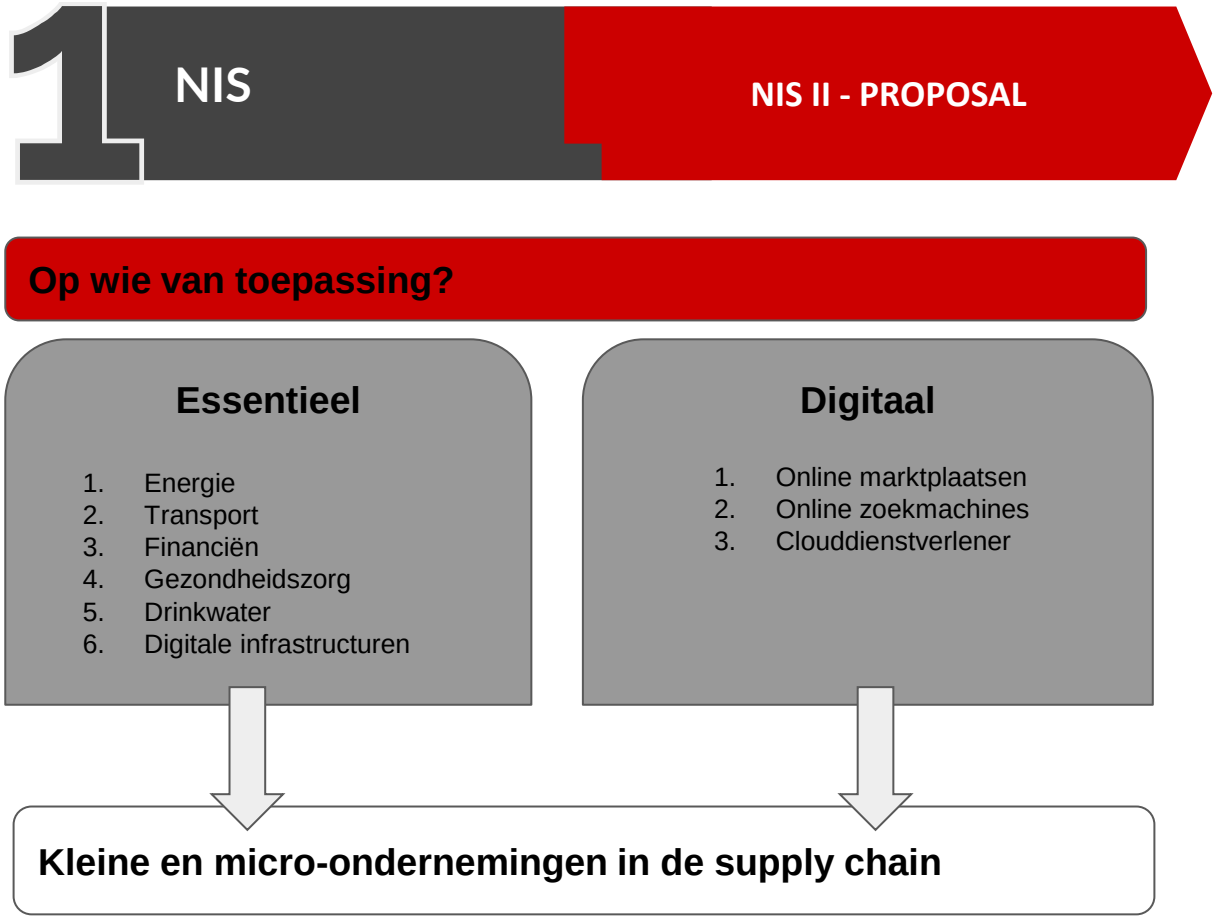
1. Energie
2. Transport
3. Financiën
4. Gezondheidszorg
5. Drinkwater
6. Digitale infrastructuren

Digitaal

1. Online marktplaatsen
2. Online zoekmachines
3. Clouddienstverlener

Kleine en micro-ondernemingen in de supply chain

Cyber resilience



Cyber resilience

Verplichtingen? (vb. digitale dienstverleners)

Beveiliging

Melding

Informatie

Cyber resilience

1 NIS

Verplichtingen? (vb. digitale dienstverleners)

		Sancties
Beveiliging	→	SR: 8d-1j gs / 208 tot 240.000 euro gb AR: 500 tot 100.000 gb
Melding	→	SR: 8d-1j gs / 208 tot 160.000 euro gb AR: 500 tot 75.000 gb
Informatie	→	SR: 8d-1j gs / 208 tot 400.000 euro gb AR: 500 tot 75.000 gb

Cyber resilience

1 NIS

CENTRE FOR CYBER SECURITY BELGIUM

ccb.belgium.be

CYBER SECURITY COALITION.be

cybersecuritycoalition.be

Cyber resilience

2 Cyber Security Act

→ Versterking positie

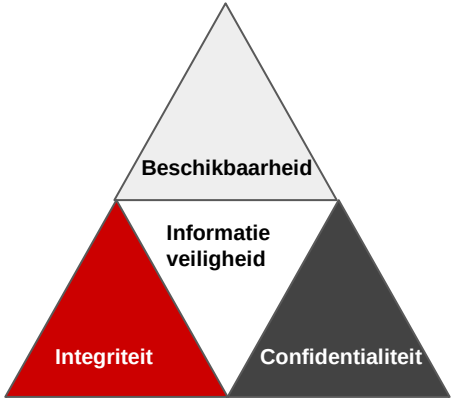
→ Europees kader voor ICT-producten, - diensten en -processen

3 GDPR

Preambule 49:
verwerking met oog op beveiliging = gerechtvaardigd belang

Art. 5:
Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (“integriteit en vertrouwelijkheid”)

Art. 32:
passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen



CIA-triad

3 GDPR

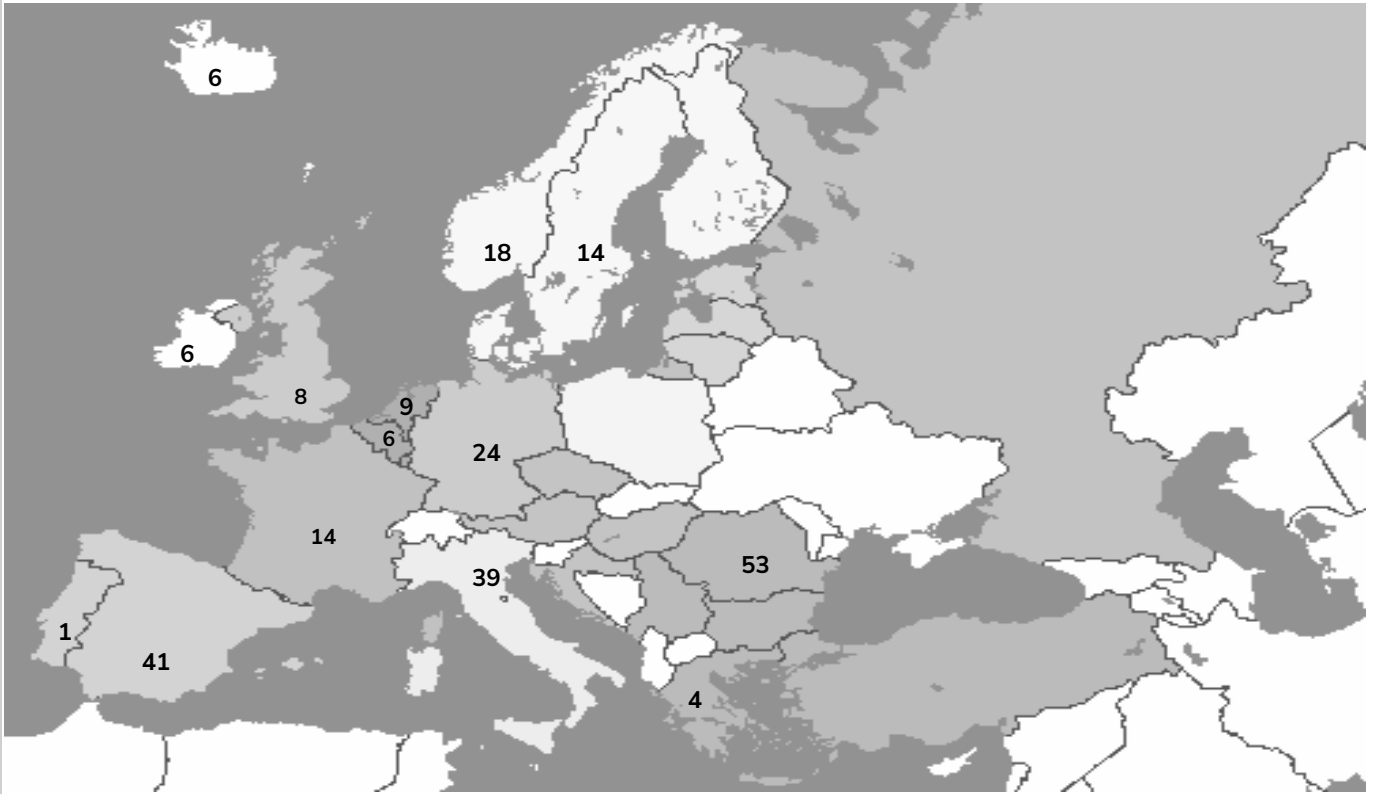
Praktijkvoorbeelden

ICO/Marriott-hotels (30/10/2020)
Trojan malware - onvoldoende monitoring, onvoldoende control en te beperkte encryptie - 18,4 miljoen pond boete

ICO/British Airways (16/10/2020)
Hack + link naar frauduleuze site - onvoldoende veiligheid (geen multi factor authenticatie), onvoldoende awareness - 20 miljoen pond boete

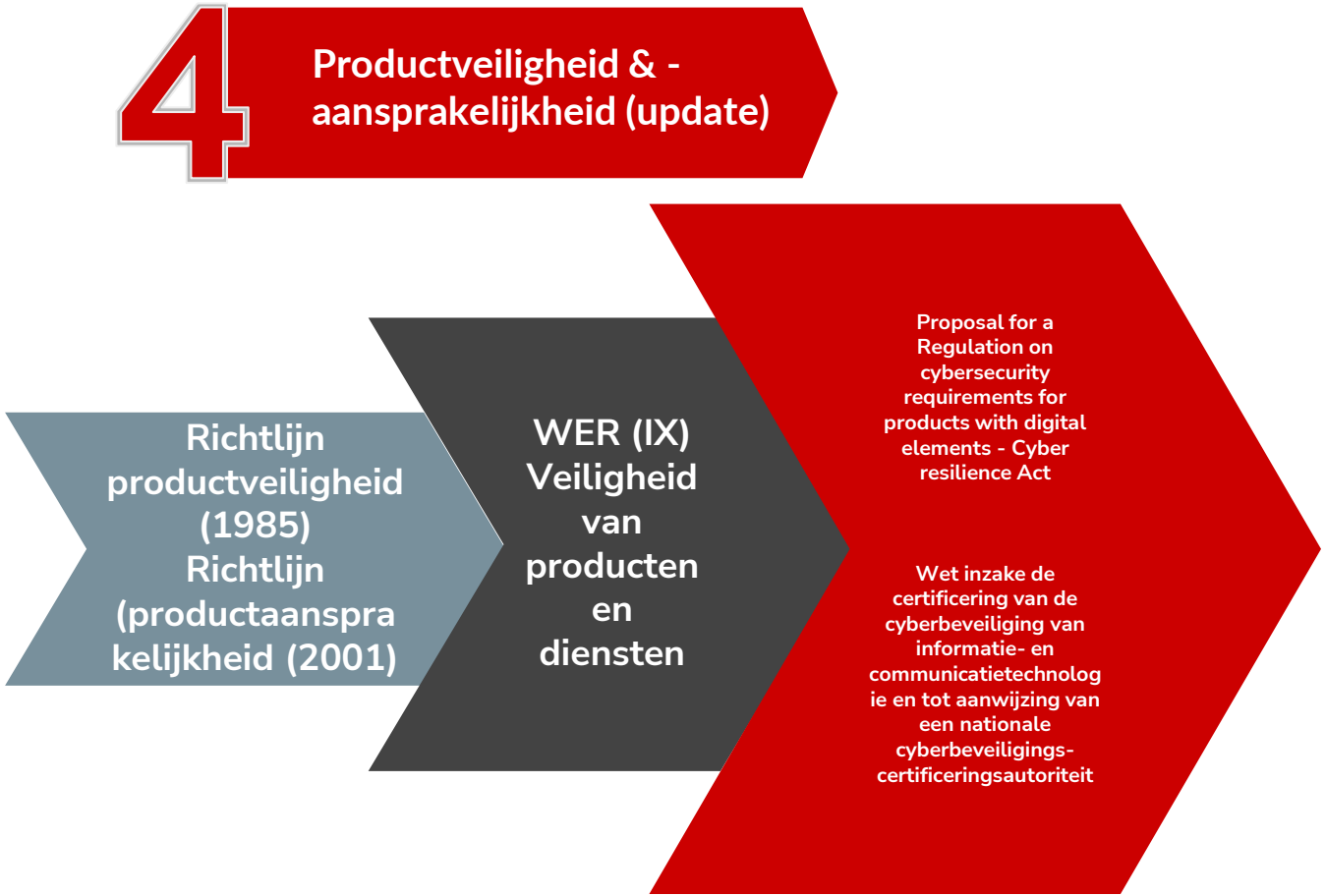
Cyber resilience

Onvoldoende maatregelen onder GDPR



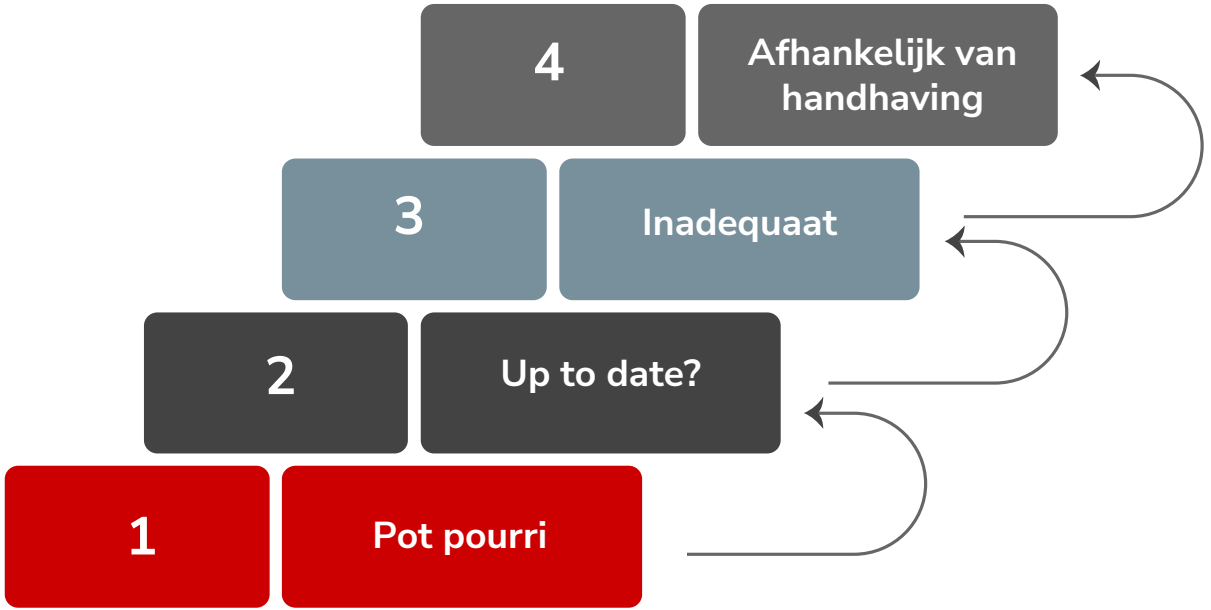
NCOI M&D Seminars

Cyber resilience



Cyber resilience

Belgisch recht?

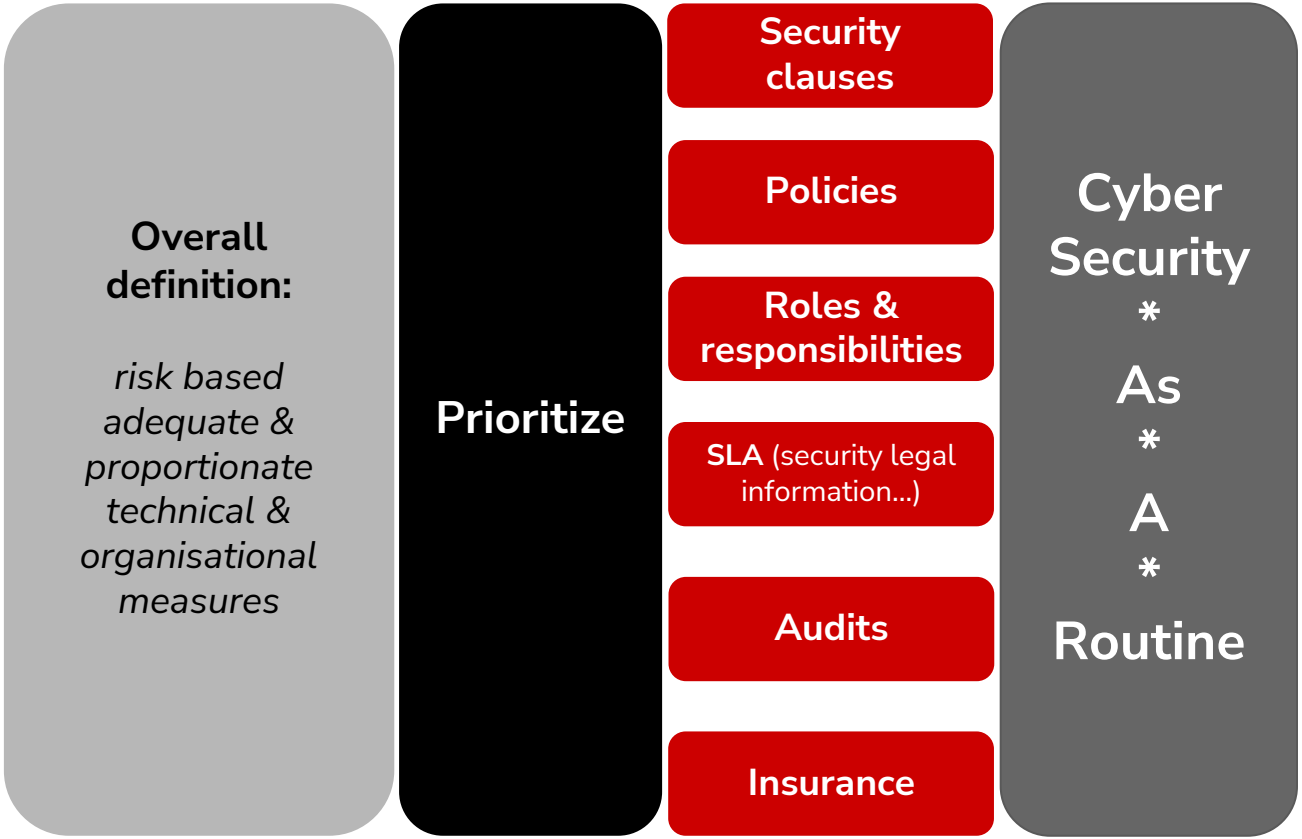


Cyber security =
secure
accountability

National Institute of Standards and Technology
U.S. Department of Commerce

Identify =	Risk assessments & audits
Protect =	Organisational & technical measures
Detect =	Monitoring & logging
React =	Incident Response Management
Recover =	Claim handling, cost allocation

Secure accountability



Secure accountability

Het menselijke aspect bij cyberbeveiliging…

Europese commissie (2017): *95% van de cyberincidenten wordt mogelijk gemaakt door een of andere menselijke fout*

Rapport Enisa (2018): Gedragsaspecten van cybersecurity

- Zwakste schakel
- Techniek in harmonie met de mens
- Gebrek tijd & middelen
- Vaardigheden + herstructurering praktijk en beleid
- balans tussen productiviteit en veiligheid

Shadow-IT

Werkgever = steeds aansprakelijk

- **Art. 32 (4) GDPR**: *De verwerkingsverantwoordelijke en de verwerker **treffen maatregelen** om ervoor te zorgen dat **iedere natuurlijke persoon** die handelt **onder het gezag** van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze **slechts in opdracht van de verwerkingsverantwoordelijke verwerkt**,..*
- **Art. 29 GDPR**: *De verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze **uitsluitend in opdracht** van de verwerkingsverantwoordelijke,..*
- **Art. 82 (3) GDPR**: *Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld **indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.***

Shadow-IT

… maar de werknemer gaat niet vrijuit!

Arbeidsovereenkomstenwet: werknemer niet aansprakelijk, tenzij bedrog of zware schuld

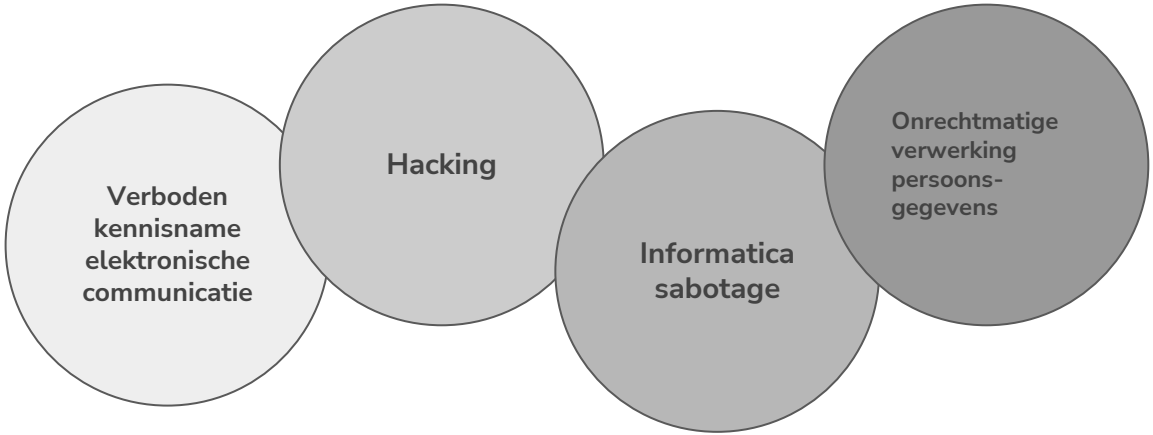
Schending regel O.O. = zware schuld

GDPR-wet
- = O.O. (want strafrechtelijke sancties)
- art. 222: boete van 2.000 euro tot 120.000 Euro wegens schending principes verwerking persoonsgegevens (herinner art. 5) en de rechtmatige verwerking.
- **Wie?** *De verwerkingsverantwoordelijke of de verwerker, zijn **aangestelde of gemachtigde**…*

E-mails & andere datasystemen

Wie heeft toegang tot wat?

Slechte rolverdeling en gebrek aan interne afspraken verhogen het risico op:



Pentesting & Coordinated vulnerability disclosure

Vrijwillig (laten) hacken?

Waardevolle aanvulling op je securitybeleid:

- juridisch kader
- preventie kwetsbaarheden opzoeken
- vertrouwen bouwen
- compliancy
- vertrouwelijkheid én informatiedeling

Pentesting & Coordinated vulnerability disclosure

Vrijwillig (laten) hacken?

Waardevolle aanvulling op je securitybeleid:

- juridisch kader
- preventie kwetsbaarheden opzoeken
- vertrouwen bouwen
- compliancy
- vertrouwelijkheid én informatiedeling

Aandachtspunten:

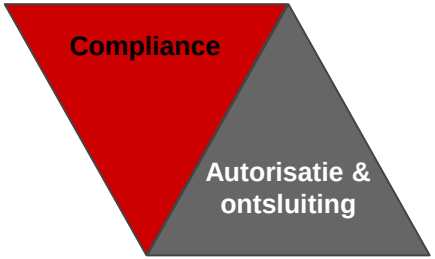
- scope en voorwaarden
- belangen derden
- gevolgen en ev. schade
- proportionaliteit
- GDPR...
- geen stand-alone

Secure accountability

Kwaliteit & veiligheid

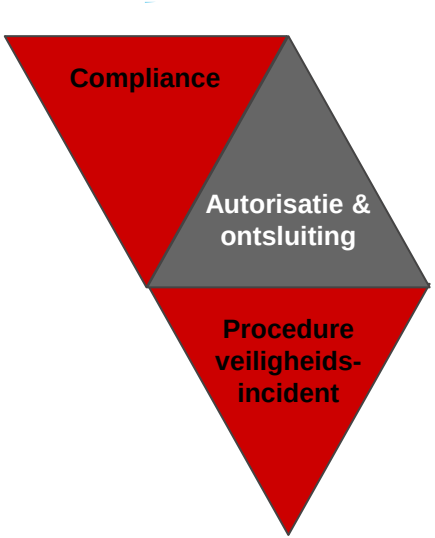
Secure accountability

Kwaliteit & veiligheid



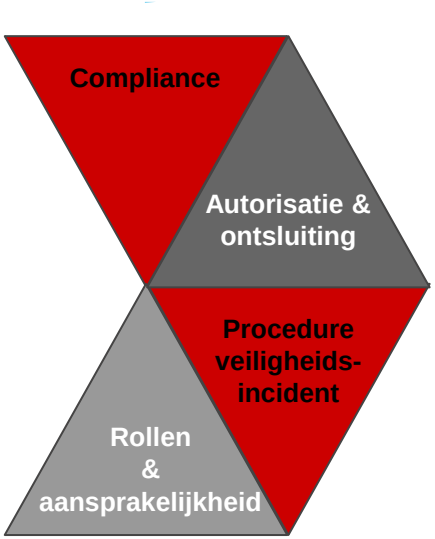
Secure accountability

Kwaliteit & veiligheid



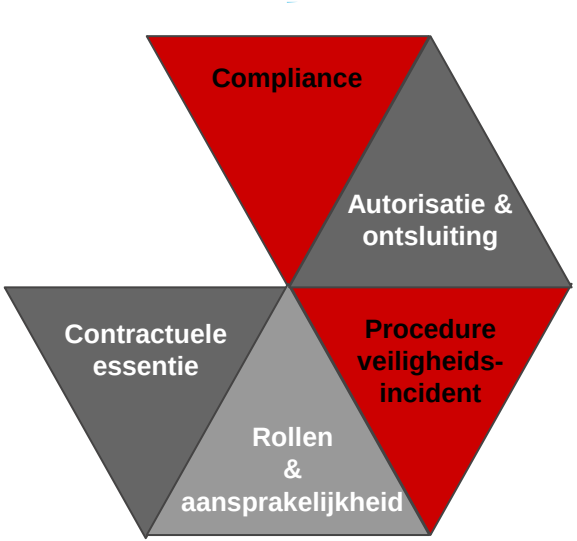
Secure accountability

Kwaliteit & veiligheid



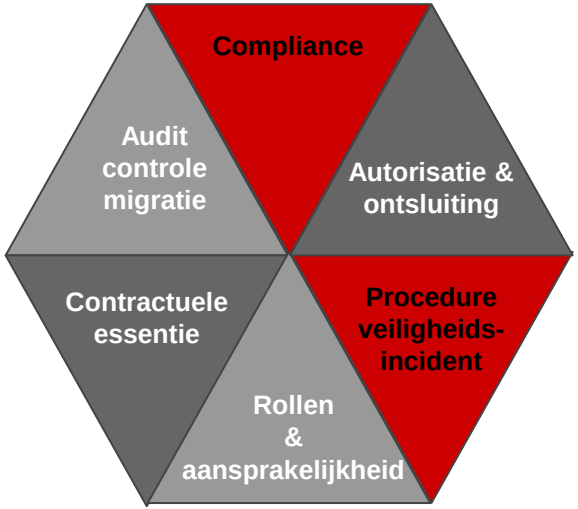
Secure accountability

Kwaliteit & veiligheid

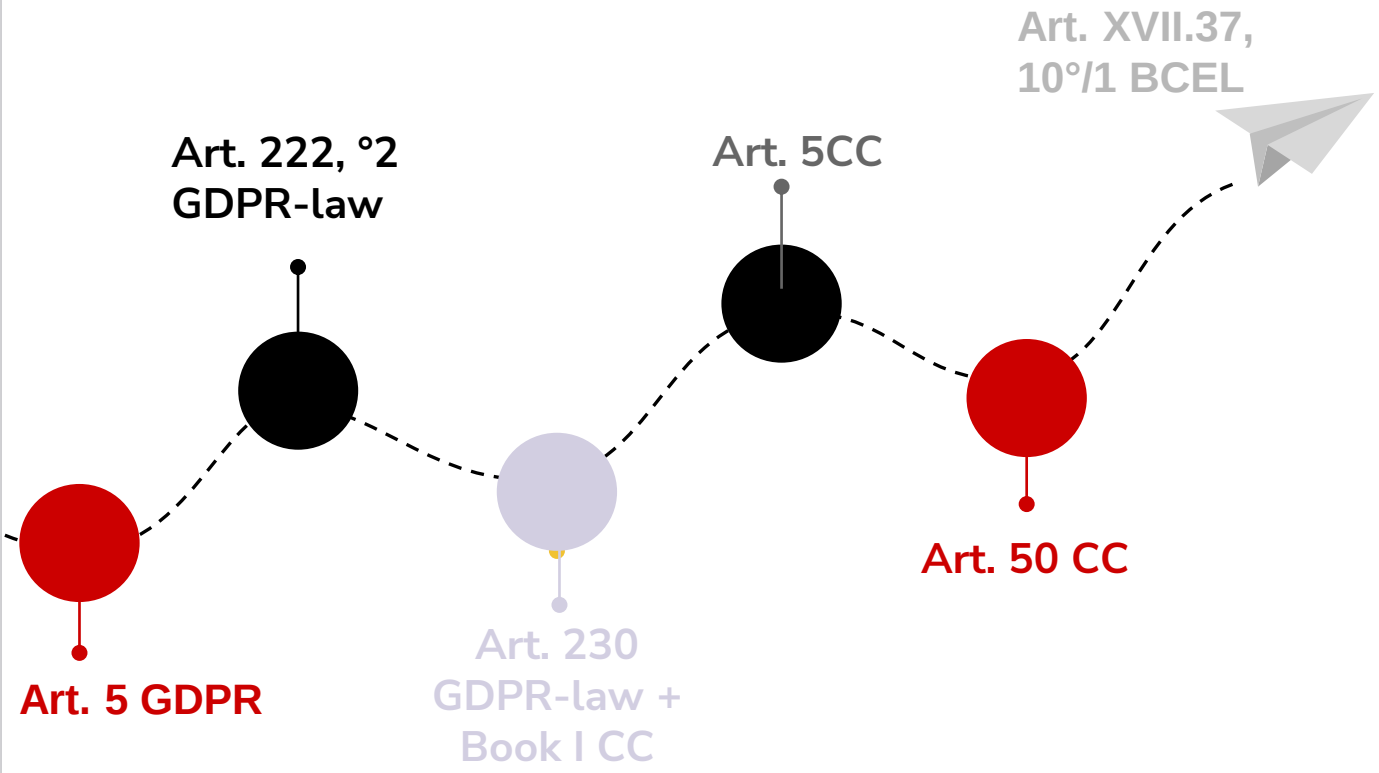


Secure accountability

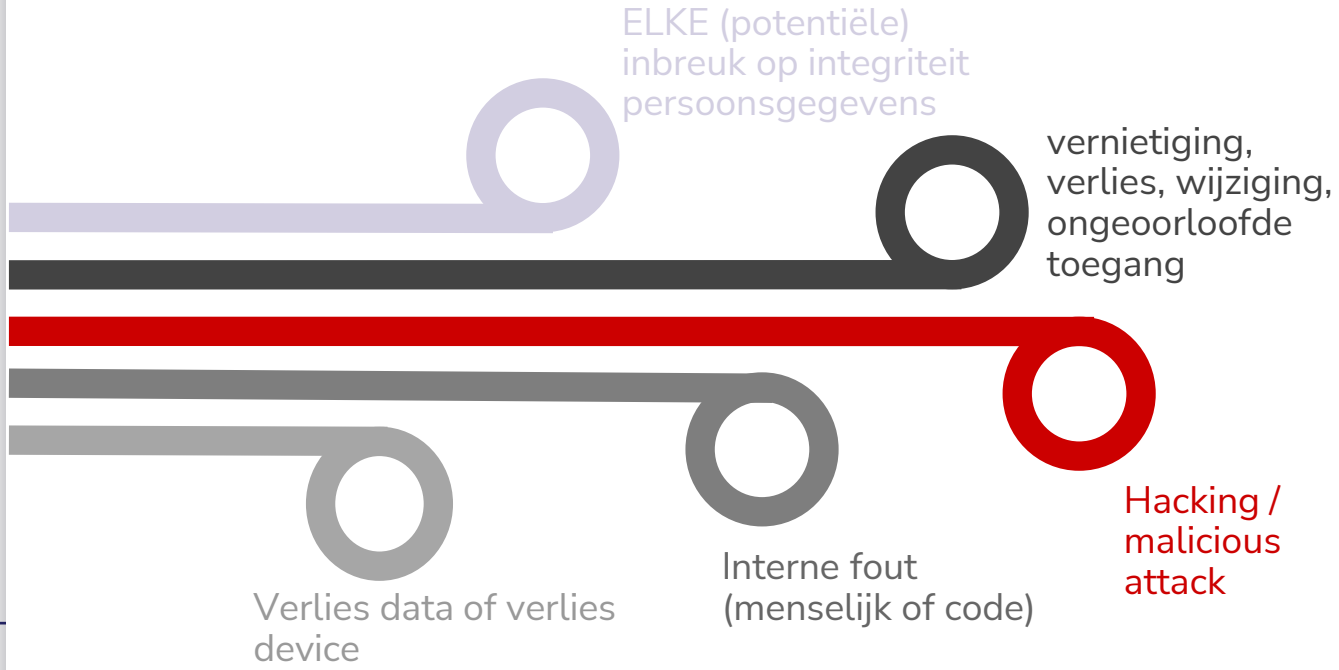
Kwaliteit & veiligheid



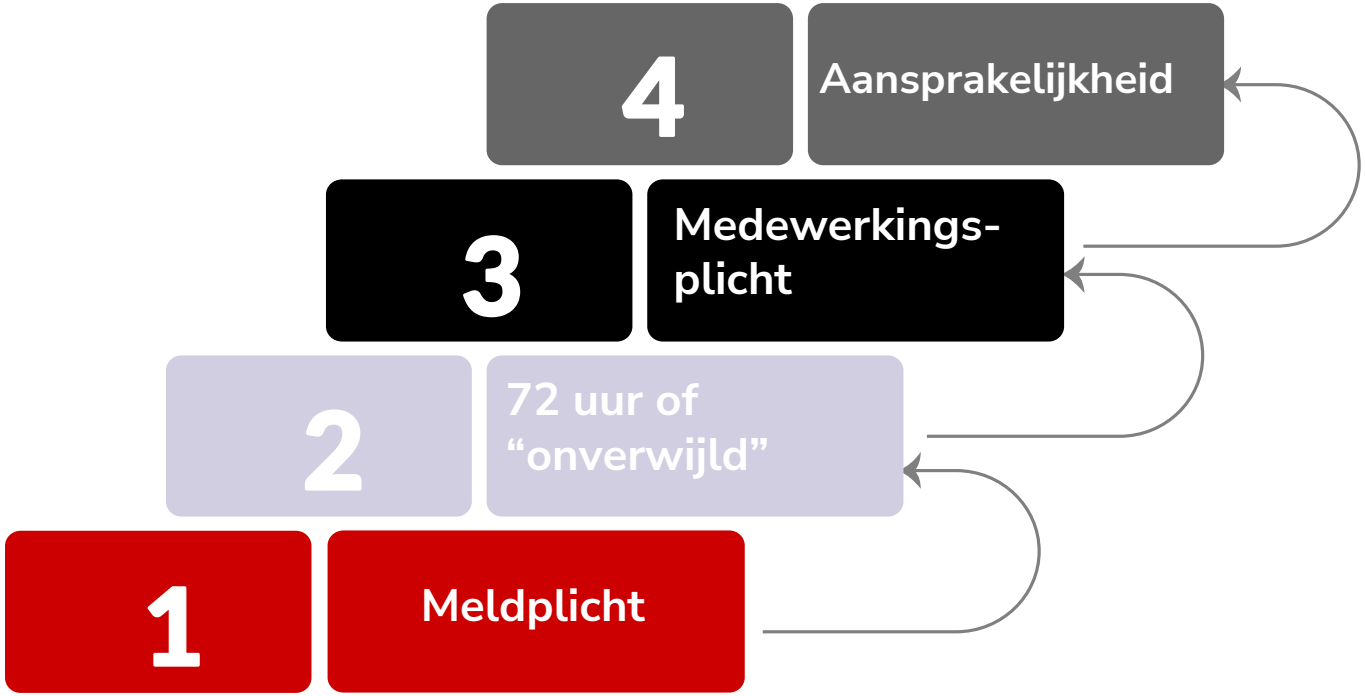
Secure accountability



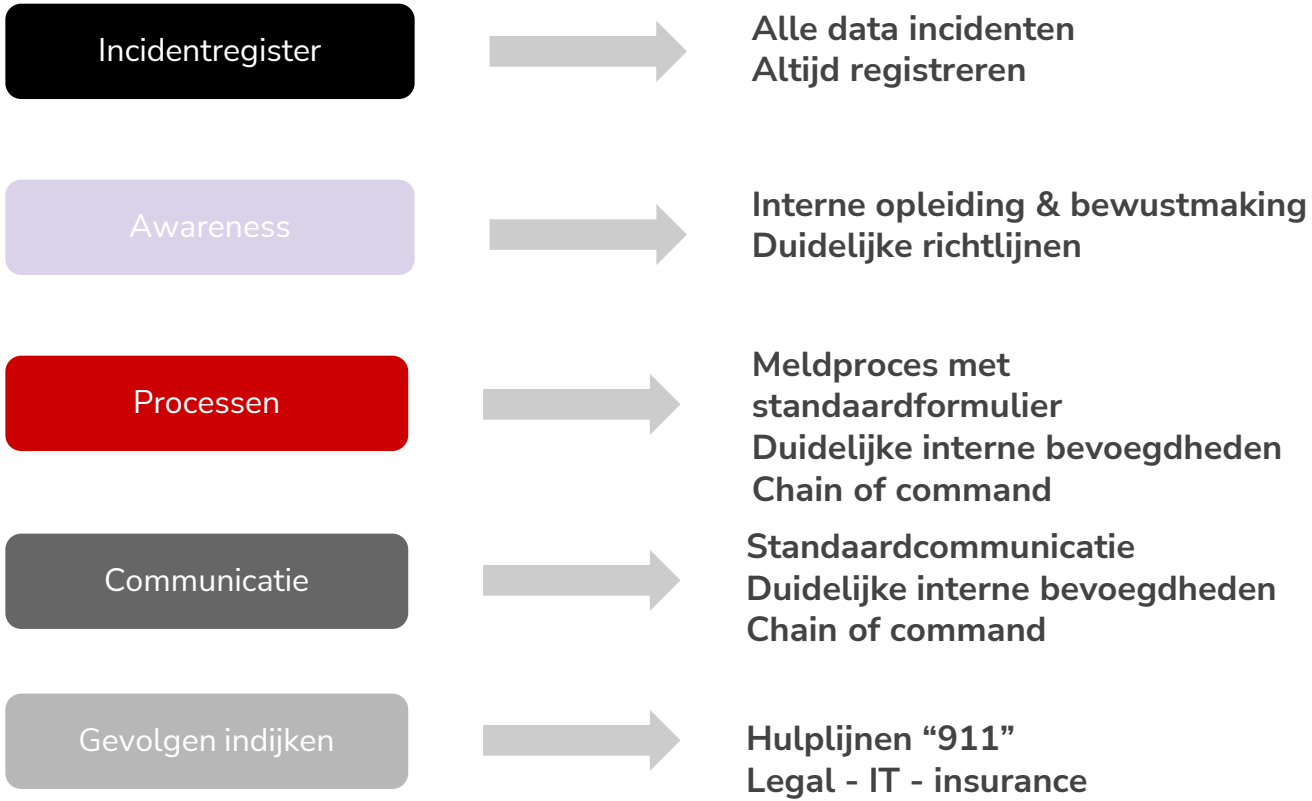
Secure accountability



Secure accountability



Secure accountability



Sirius Legal in cybersecurity

Zoek hier jouw extern advies

Agentschap Innoveren & Ondernemen (VLAIO) wenst met de cybersecurity verbetertrajecten steun te geven voor het inkopen van extern advies en begeleiding die je nodig hebt om een impuls te geven aan de cybersecurity maturiteit van jouw bedrijf.

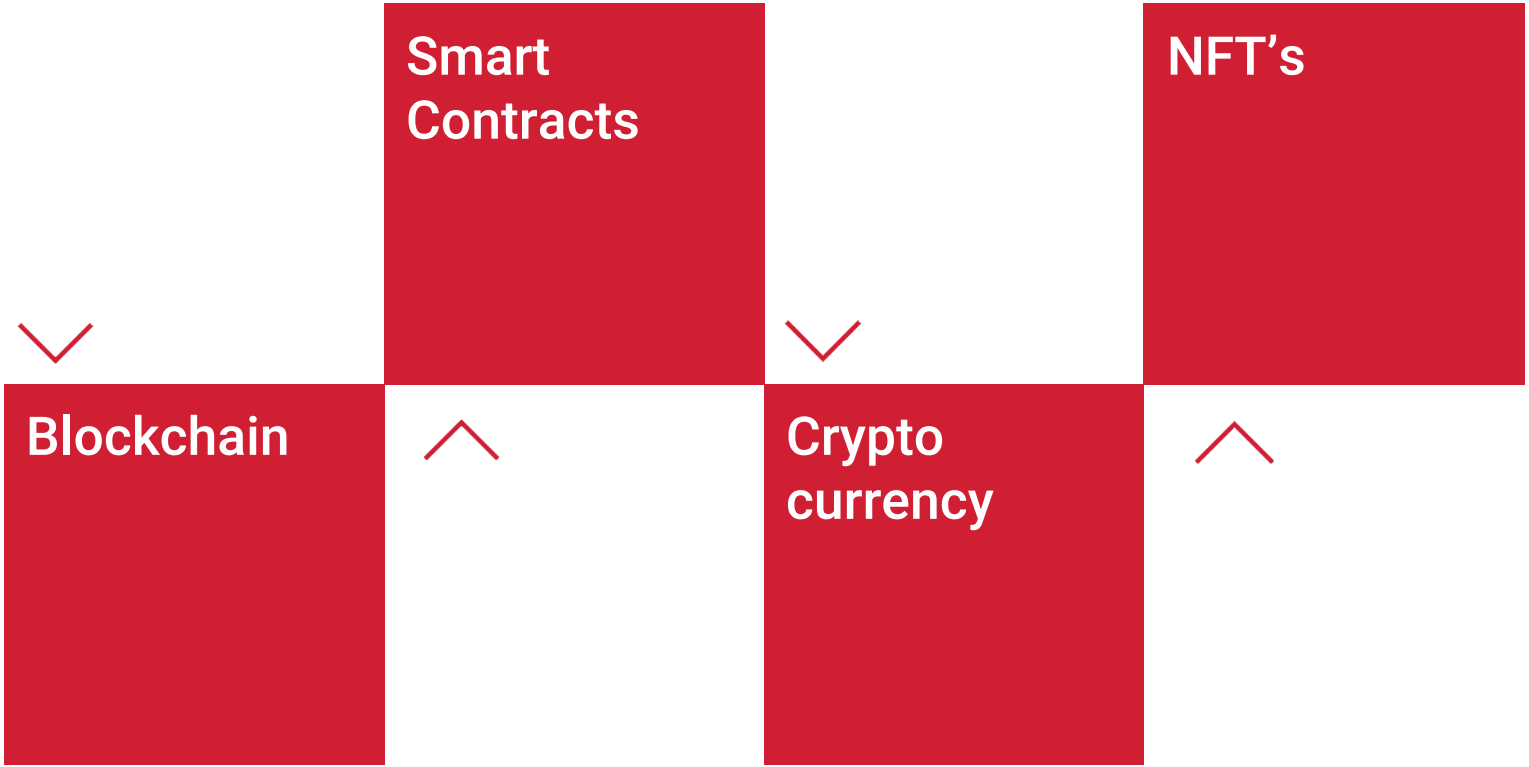
Je werkt hiervoor samen met één van deze negen geselecteerde dienstverleners. Klik door naar hun aanbod!

- BA en Sirius Legal
- Cranium Belgium
- Cronos Public Services
- EY Advisory Services
- Netcure
- NVISO Belgium
- PwC Enterprise Advisory
- Resilient
- Toreon

AGENTSCHAP INNOVEREN & ONDERNEMEN

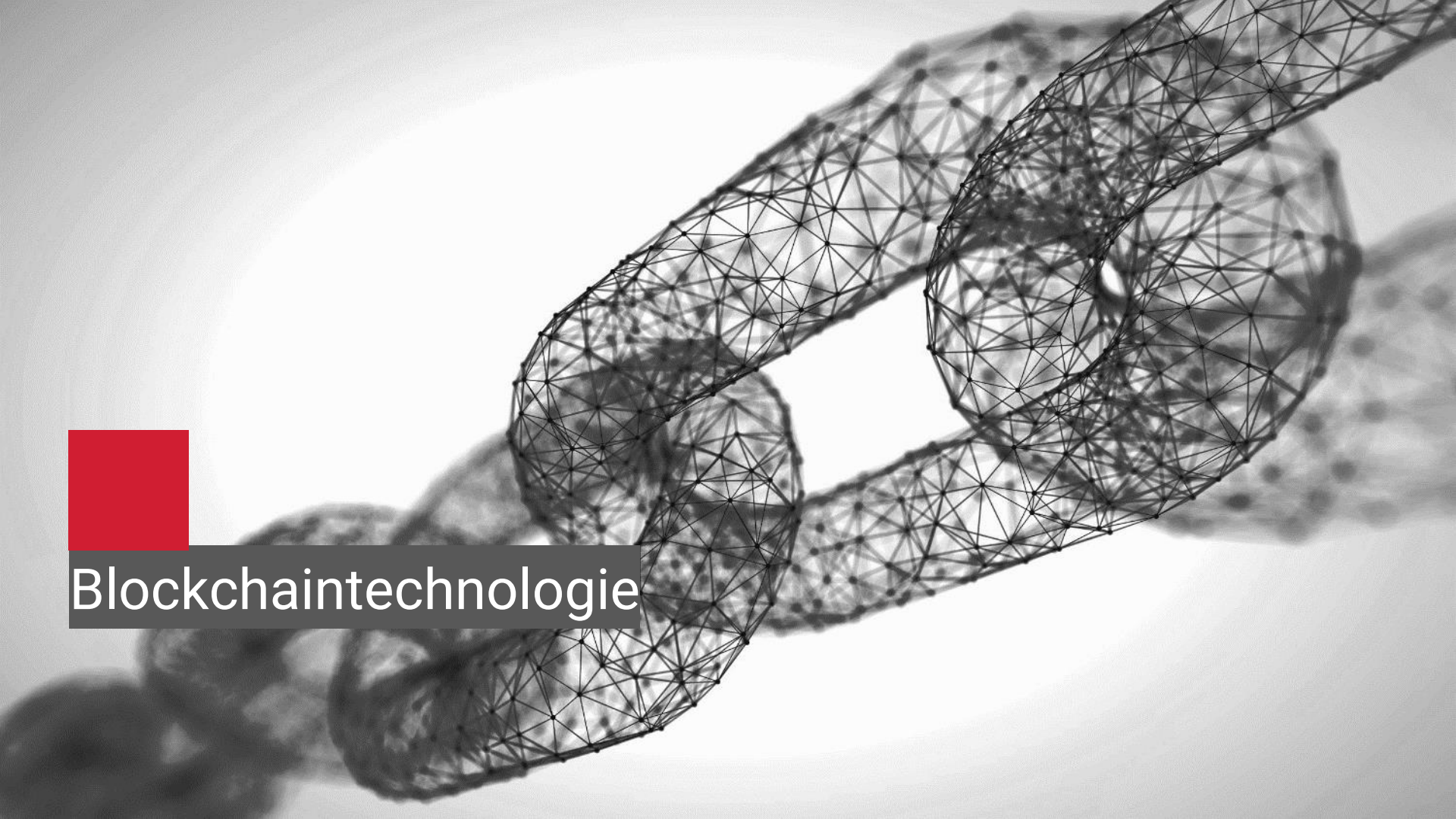
Vlaanderen is ondernemen

SIRIUS.LEGAL
BUSINESS LAW FIRM
Blockchain
Smart Contracts
Cryptocurrency
NFT’s


Smart Contracts
NFT’s
Blockchain
Crypto currency

4 totaal verschillende concepten
Zowel technologisch als juridisch
Maar...

Blockchaintechnologie



“Blockchain was invented in 2008 by Satoshi Nakamoto to serve as the public transaction ledger for the first cryptocurrency Bitcoin”.

Niet dus, dit is één van die hardnekkige internetmythes

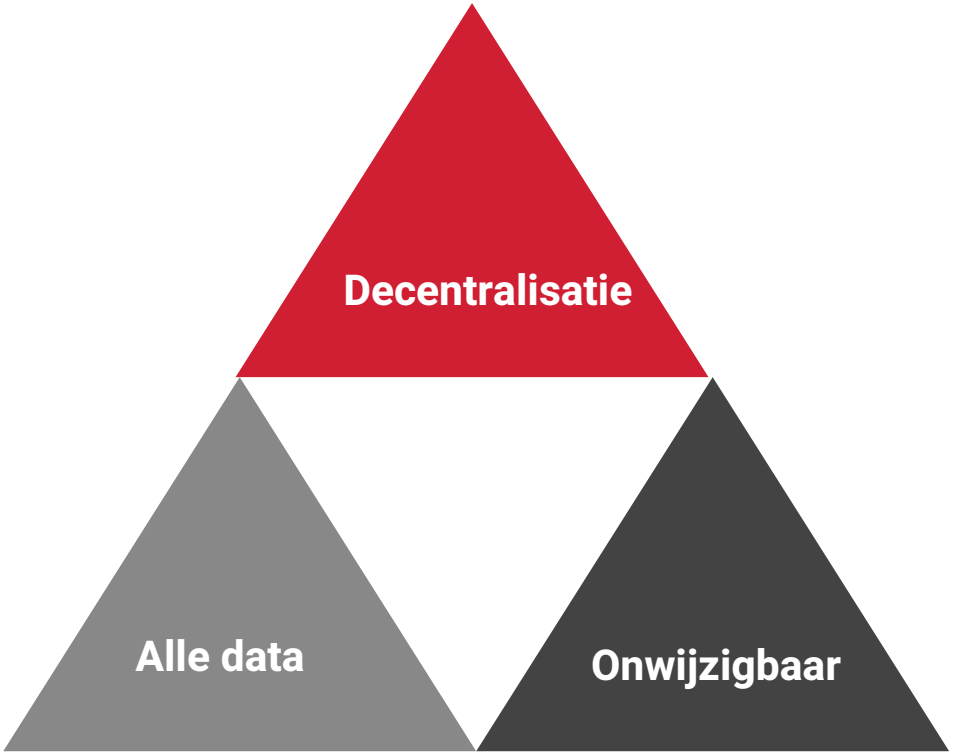
Onderliggende technologie bestaat als sinds begin van de jaren 90

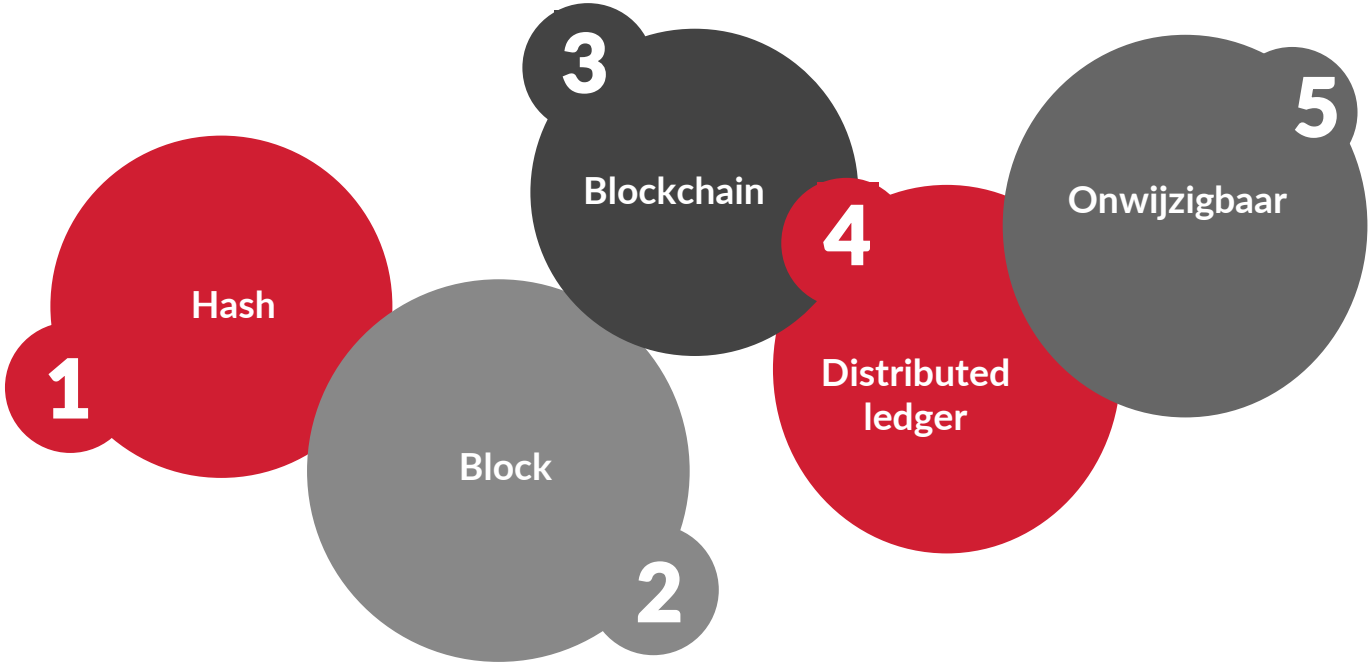
Maar bleef jarenlang quasi onopgemerkt

Tot Bitcoin op de proppen kwam

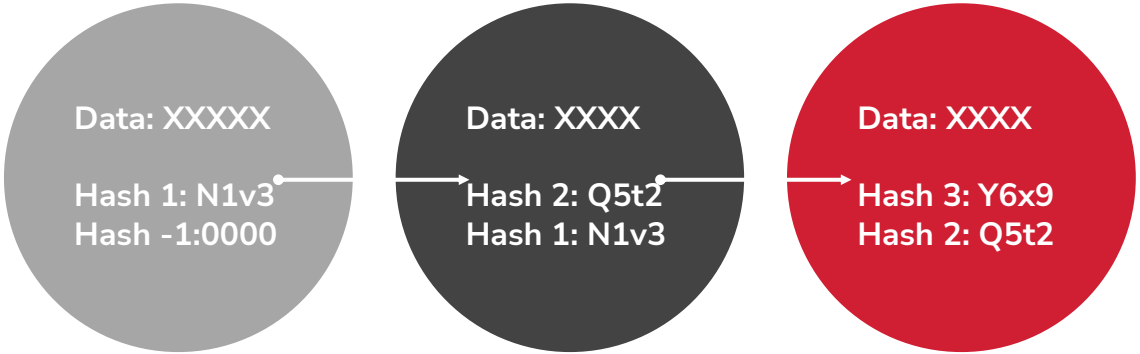
Maar blockchain is zoveel méér dan bitcoin en cryptocurrencies...

“Blockchain is een gedistribueerde opslagtechnologie die alle mogelijke soorten data op in een P2P netwerk onwijzigbaar opslaat”

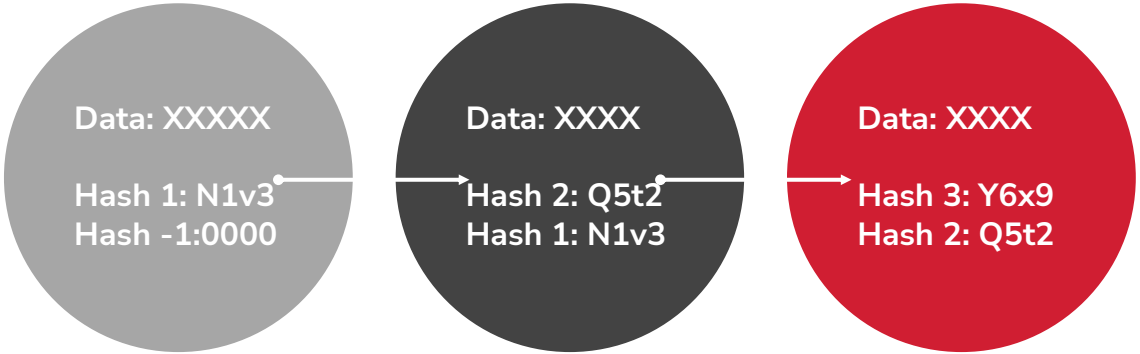


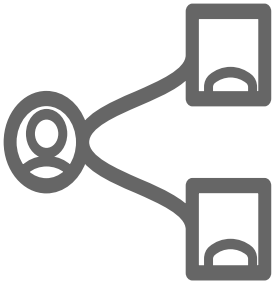

1
Hash
2
Block
3
Blockchain
4
Distributed ledger
5
Onwijzigbaar

Hash - Block - Chain

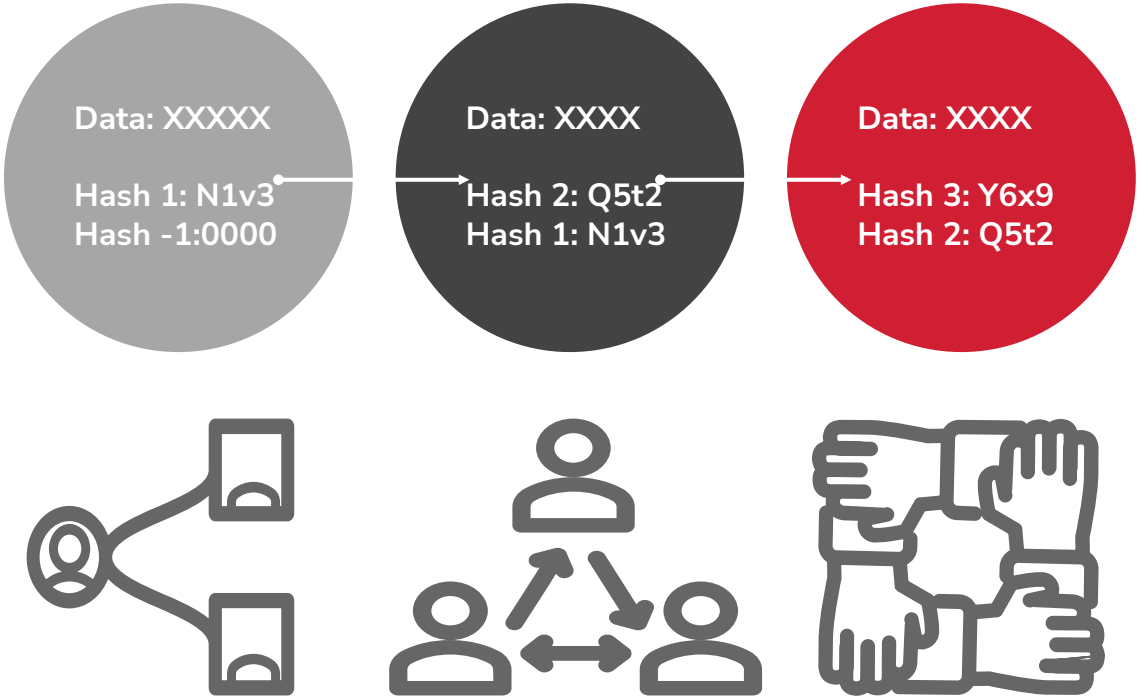


Hash - Block - Chain - Gedecentraliseerd

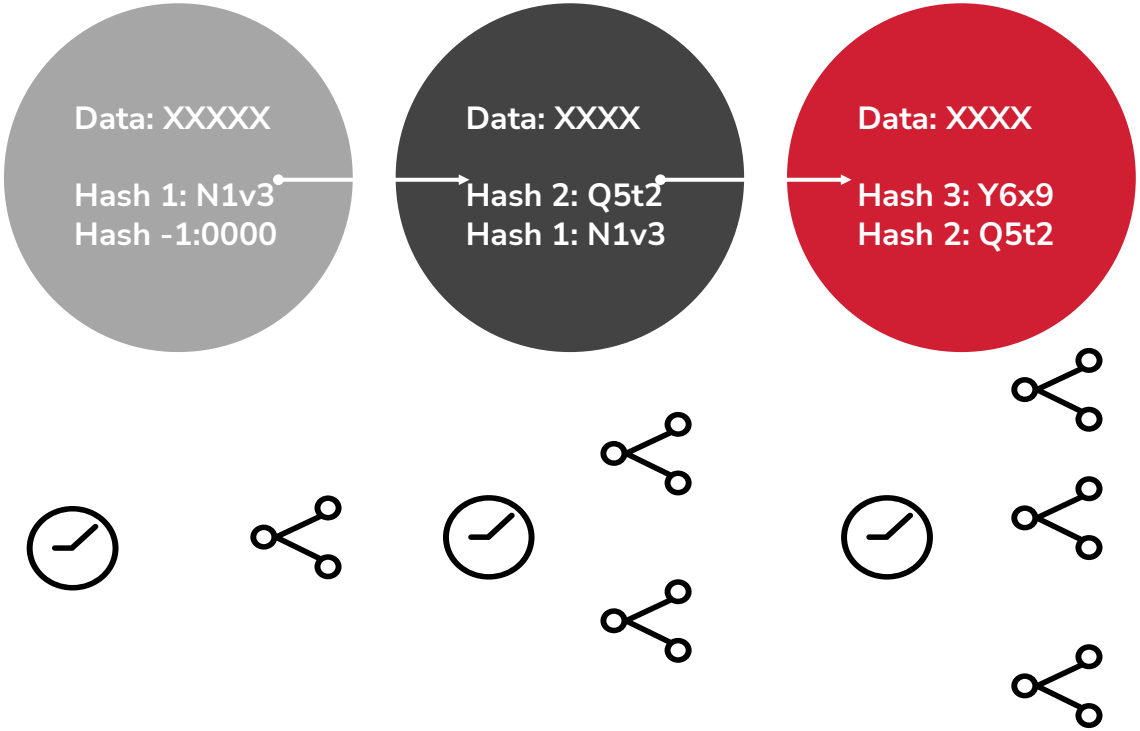




Hash - Block - Chain - Gedecentraliseerd



Hash - Block - Chain - Gedecentraliseerd - Onwijzigbaar



Privaat vs. Publiek

Private blockchain	▪ Enkel goedgekeurde users ▪ Niet iedereen kan data toevoegen of wijzigen ▪ Identificatie en controle van users mogelijk
Publieke blockchain	▪ Open voor iedereen ▪ Iedereen kan data toevoegen of wijzigen ▪ Anoniem (met alle gevolgen vandien)

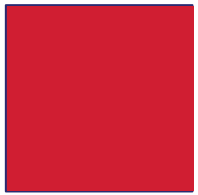
Use Case:

Maersk international container transport

Use Case:

EUIPO connects to TMview and DesignView through blockchain

Use cases



Cryptocurrencies

Kadaster - vastgoedregister

BTW
Inkomstenbelasting
Vennootschapsbelasting
...

Aandeelhoudersregisters
UBO

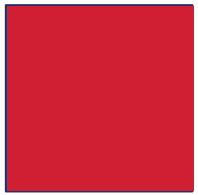
Internationale betalingen

IP Rights management

Contract management

NFT's

Use cases



Cryptocurrencies

Kadaster - vastgoedregister

BTW
Inkomstenbelasting
Vennootschapsbelasting
...

Aandeelhoudersregisters
UBO

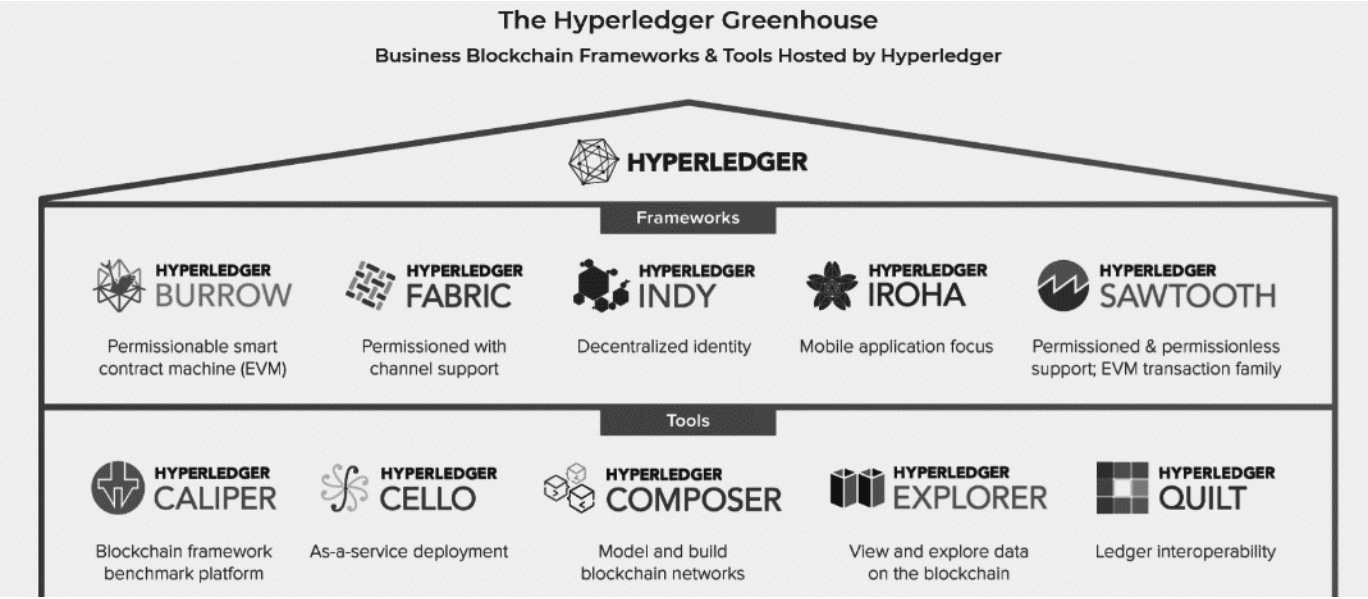
Internationale betalingen

IP Rights management

Contract management

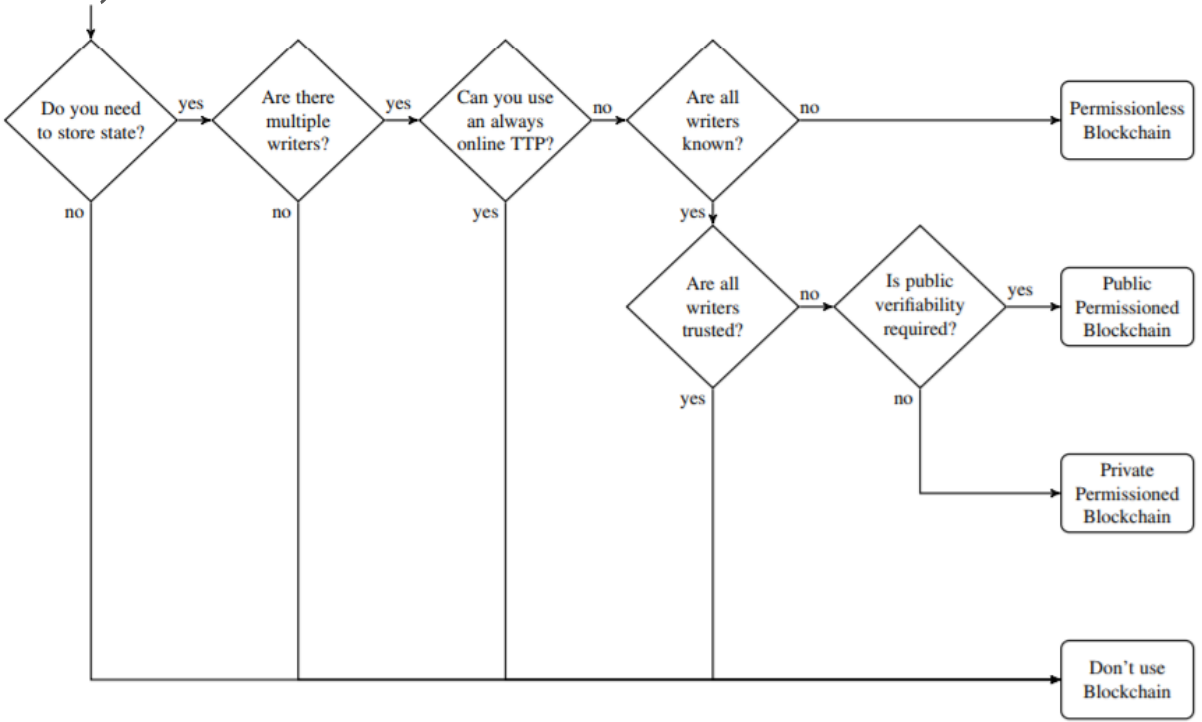
NFT's

Wie zelf aan de slag wil...

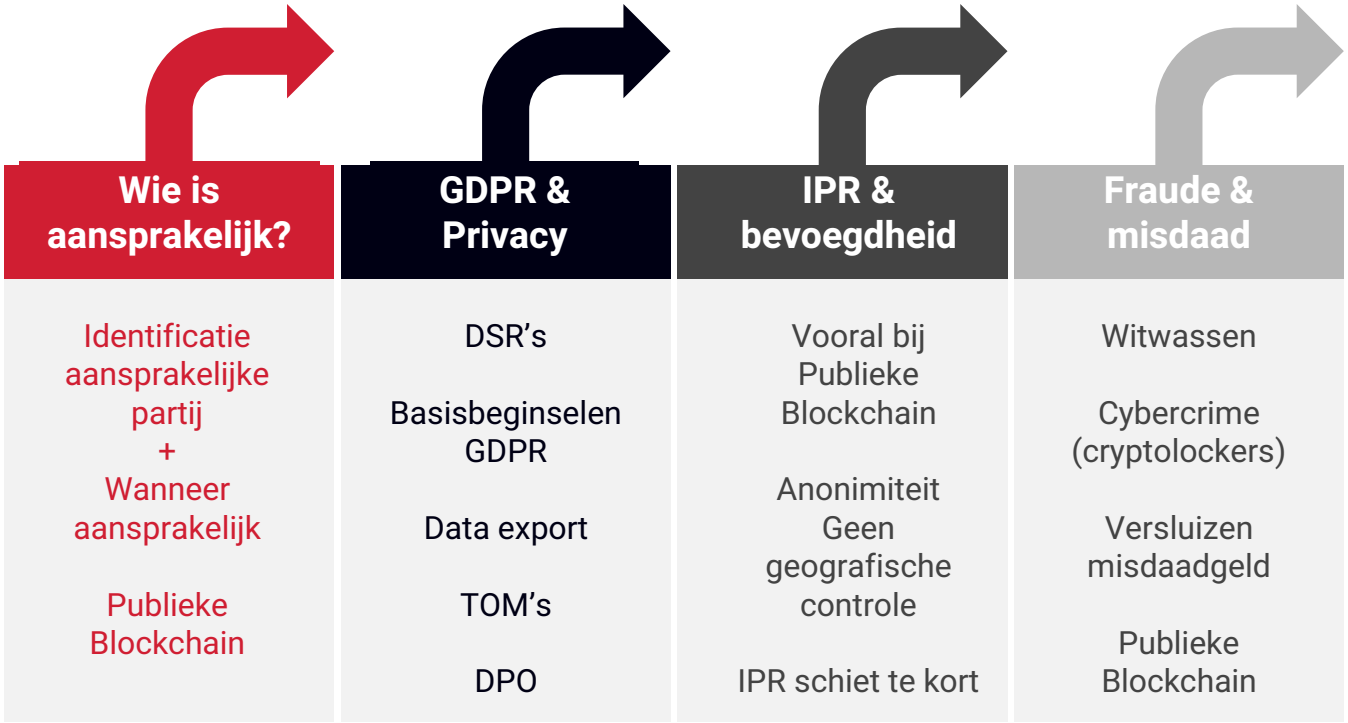


Kijk voorbij de hype

(Wüst-Gervais 2017)



Juridische uitdagingen



Smart contracts

“a computerised transaction protocol that executes the terms of a contract”
(Szabo, 1994)

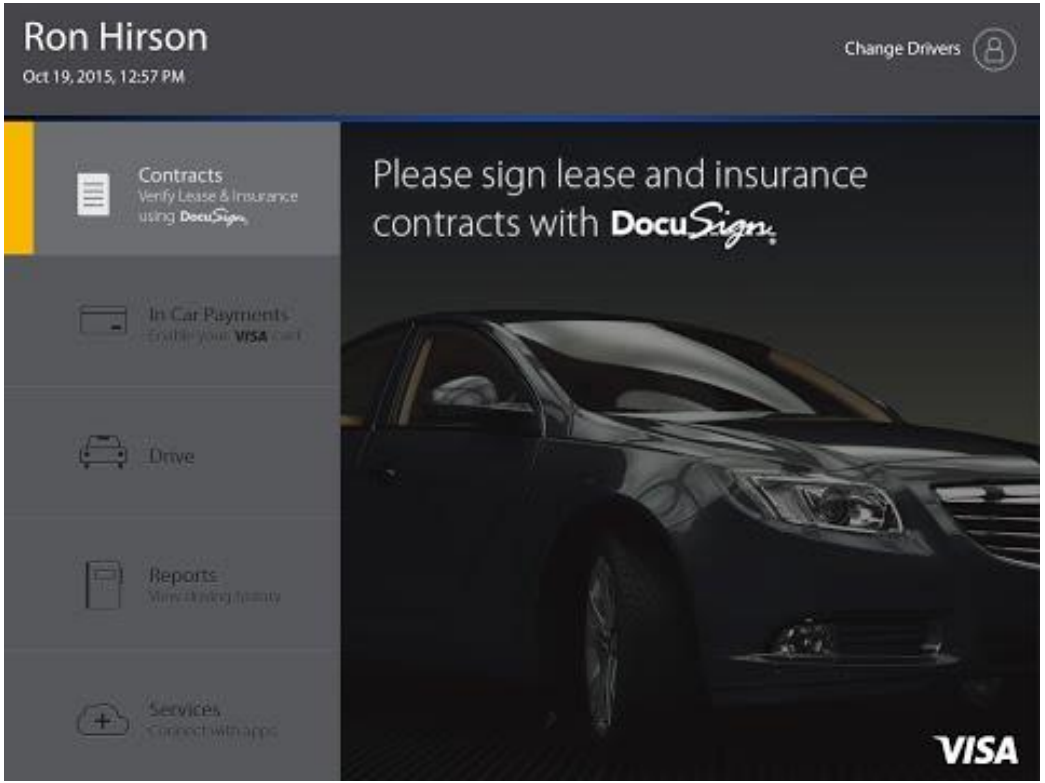
Lees: “een stuk computercode”

“Smart”
Omdat het protocol een proces kan documenteren en technisch afdwingen bij gebruikers

“Contract”
Omdat (meestal) signature vereist is en omdat protocol (minstens technisch) bindend is voor de gebruiker

"a computerised transaction protocol that executes the terms of a contract"

(Szabo, 1994)



“a computerised transaction protocol that executes the terms of a contract”

(Szabo, 1994)

“a computerised transaction protocol that executes the terms of a contract”

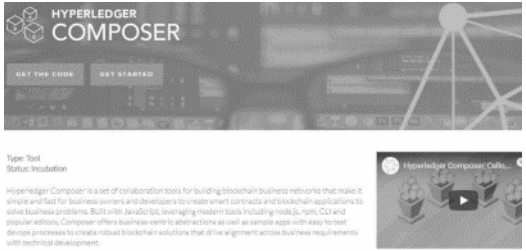
(Szabo, 1994)

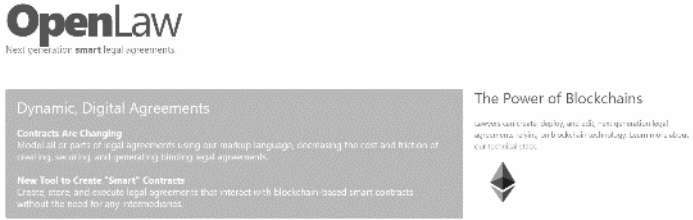
```
pragma solidity ^0.4.21;

contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    // Ensure that `msg.value` is an even number.
    // Division will truncate if it is an odd number.
    // Check via multiplication that it wasn't an odd number.
    function Purchase() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value);
    }

    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(msg.sender == buyer);
        _;
    }

    modifier onlySeller() {
        require(msg.sender == seller);
        _;
    }

    modifier inState(State _state) {
        require(state == _state);
        _;
    }
```

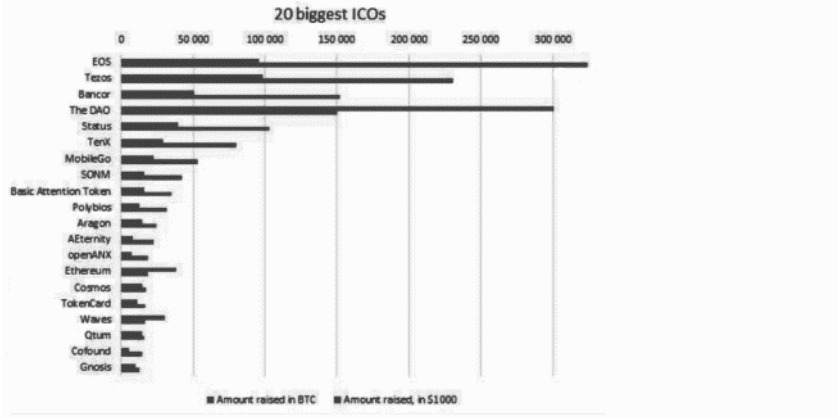
```
    event Aborted();
    event PurchaseConfirmed();
    event ItemReceived();

    /// Abort the purchase and reclaim the ether.
    /// Can only be called by the seller before
    /// the contract is locked.
    function abort()
        public
        onlySeller
        inState(State.Created)
    {
        emit Aborted();
        state = State.Inactive;
        seller.transfer(this.balance);
    }

    /// Confirm the purchase as buyer.
    /// Transaction has to include `2 * value` ether.
    /// The ether will be locked until confirmReceived
    /// is called.
    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }
```

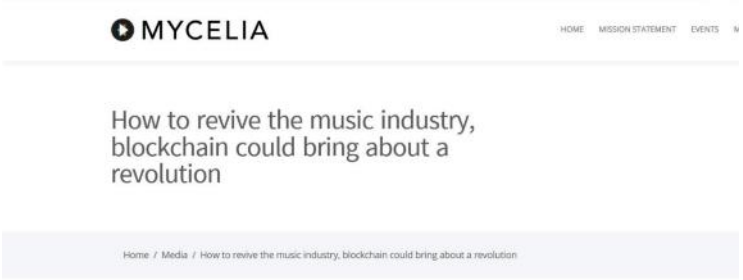
```
    /// Confirm that you (the buyer) received the item.
    /// This will release the locked ether.
    function confirmReceived()
        public
        onlyBuyer
        inState(State.Locked)
    {
        emit ItemReceived();
        // It is important to change the state first because
        // otherwise, the contracts called using `send` below
        // can call in again here.
        state = State.Inactive;

        // NOTE: This actually allows both the buyer and the seller to
        // block the refund - the withdraw pattern should be used.

        buyer.transfer(value);
        seller.transfer(this.balance);
    }
}
```

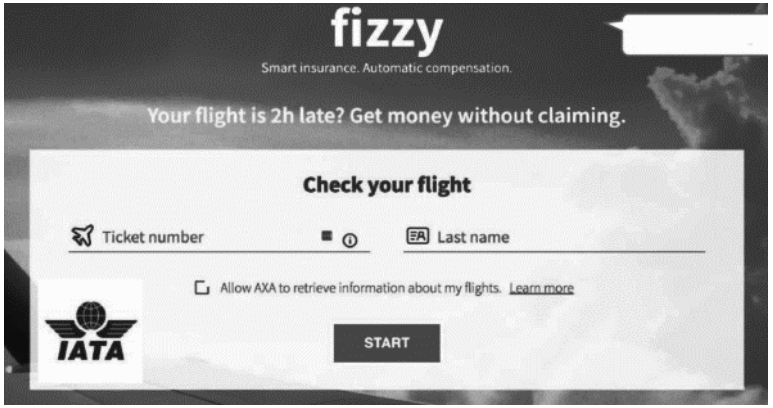
1
Proces en juridische noden worden in kaart gebracht
Taak voor jurist + business
2
Code wordt geschreven
Taak voor jurist + IT
3
Communicatie met externe data opgezet
Taak voor IT
4
Eventueel inschakelen van blockchain opslag
Taak voor IT (+ legal check)
5
Uitvoeren smart contract
Volledig automatisch
En/of taak voor business


HYPERLEDGER
COMPOSER
GET THE CODE
GET STARTED
Type: Tool
Status: Incubation
Hyperledger Composer is a set of collaboration tools for building blockchain business networks that make it simple and fast for business owners and developers to create smart contracts and blockchain applications to solve business problems. Built with JavaScript, leveraging modern tools including node.js, npm, CLI and popular editors, Composer offers business-centric abstractions as well as sample apps with easy to test, devops processes to create robust blockchain solutions that drive alignment across business requirements with technical development.
Hyperledger Composer Calls...


OpenLaw
Next generation smart legal agreements
Dynamic, Digital Agreements
Contracts Are Changing
Model all or parts of legal agreements using our markup language, decreasing the cost and friction of creating, securing, and generating binding legal agreements.
New Tool to Create "Smart" Contracts
Create, store, and execute legal agreements that interact with blockchain-based smart contracts without the need for any intermediaries.
The Power of Blockchains

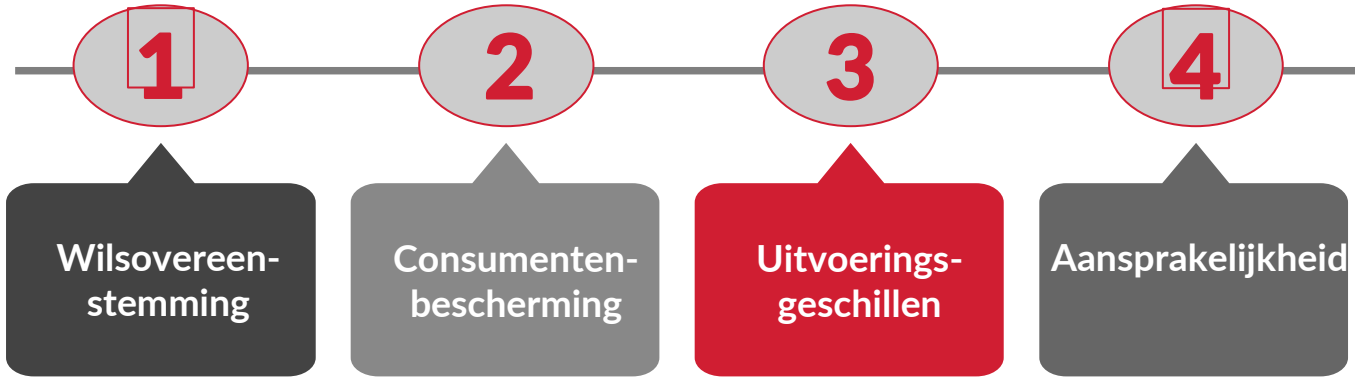

20 biggest ICOs
0
50 000
100 000
150 000
200 000
250 000
300 000
EOS
Tezos
Bancor
The DAO
Status
TenX
MobileGo
SONM
Basic Attention Token
Polybios
Aragon
AEternity
openANX
Ethereum
Cosmos
TokenCard
Waves
Qtum
Cofound
Gnosis
Amount raised in BTC
Amount raised, in $1000


MYCELIA
HOME
MISSION STATEMENT
EVENTS
How to revive the music industry, blockchain could bring about a revolution
Home / Media / How to revive the music industry, blockchain could bring about a revolution


fizzy
Smart insurance. Automatic compensation.
Your flight is 2h late? Get money without claiming.
Check your flight
Ticket number
Last name
Allow AXA to retrieve information about my flights. Learn more
START
IATA

Technische uitdagingen

Juridische uitdagingen

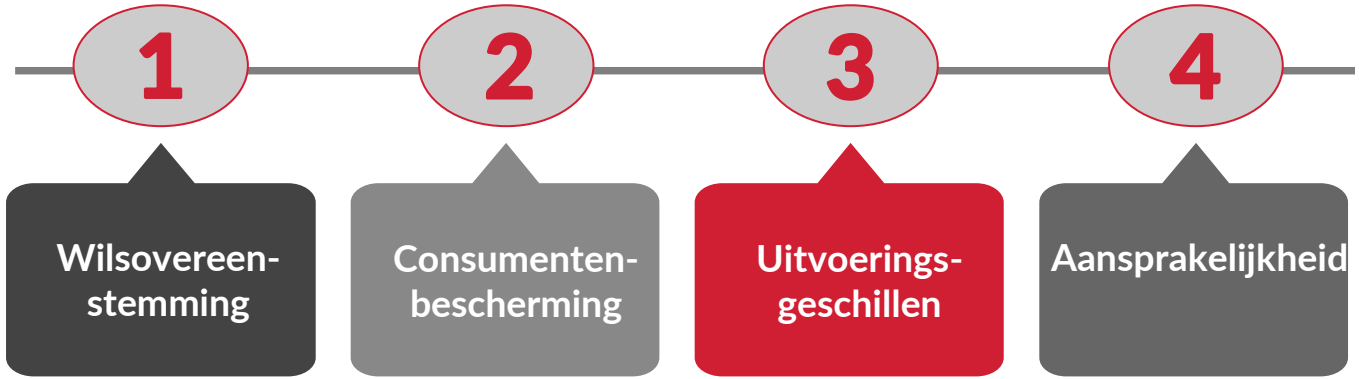


Bewijsrecht

Geldigheid wilsuiting door toetreding

“Essentiële elementen” van de overeenkomst

Vrije toestemming - wilsgebreken


1
2
3
4
Wilsovereen-stemming
Consumenten-bescherming
Uitvoerings-geschillen
Aansprakelijkheid

Eerlijke marktpraktijken

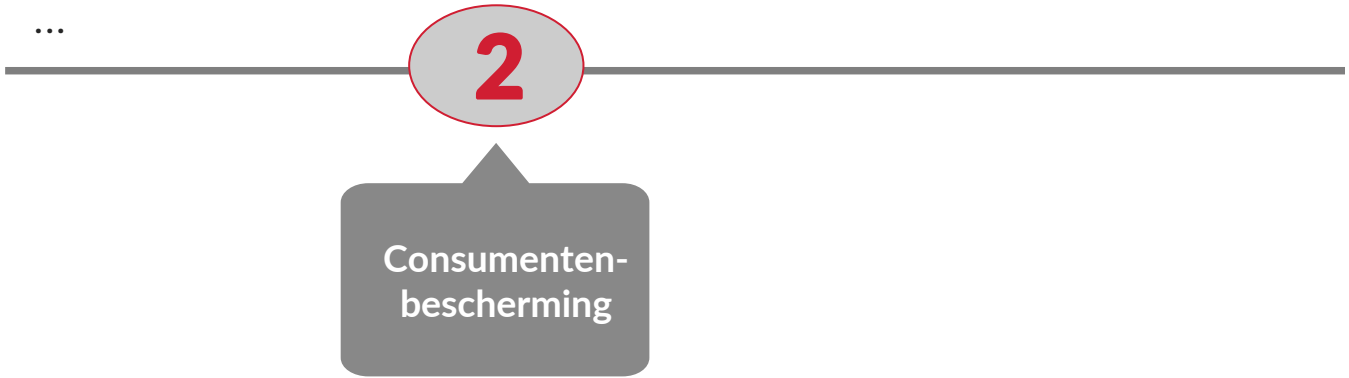
Informatieverplichtingen

Verboden bedingen

Toetredingscontracten

Verkoop op afstand

...



Overmacht

Automatische uitvoering vs. Enac

IPR - Bevoegde rechtbank - toepasselijk recht

Traagheid van gerecht vs. onmiddellijkheid van code

Ontbinding - vernietiging vs. onwijzigbare en automatische uitvoering

Wie is aansprakelijk?

Bij fouten in de code?

Bij hacking of dataverlies?

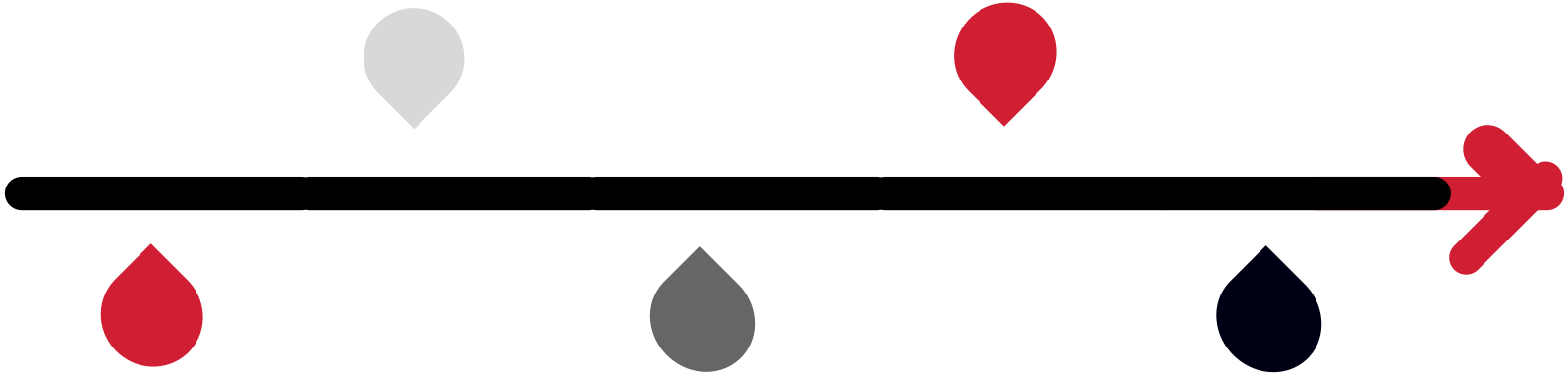
Hoe aansprakelijkheid bewijzen als consument?

1
Smart contracts zijn ideaal om probleem van vertrouwen -trust- te ondervangen
2
Smart contracts zijn geschikt voor bepaalde use case, maar niet overal inzetbaar
3
De onderliggende technologie is nog erg prematuur
4
De potentiële juridische risico's zijn erg talrijk
5
Wait for the hype to pass...

Cryptocurrencies

2009
Gestage groei en koersstijging voor Bitcoin & Ethereum, Altcoin, ...

2020
Nieuwe koersrecords
Diversificatie: payment tokens, security tokens, utility tokens, stablecoins, ...

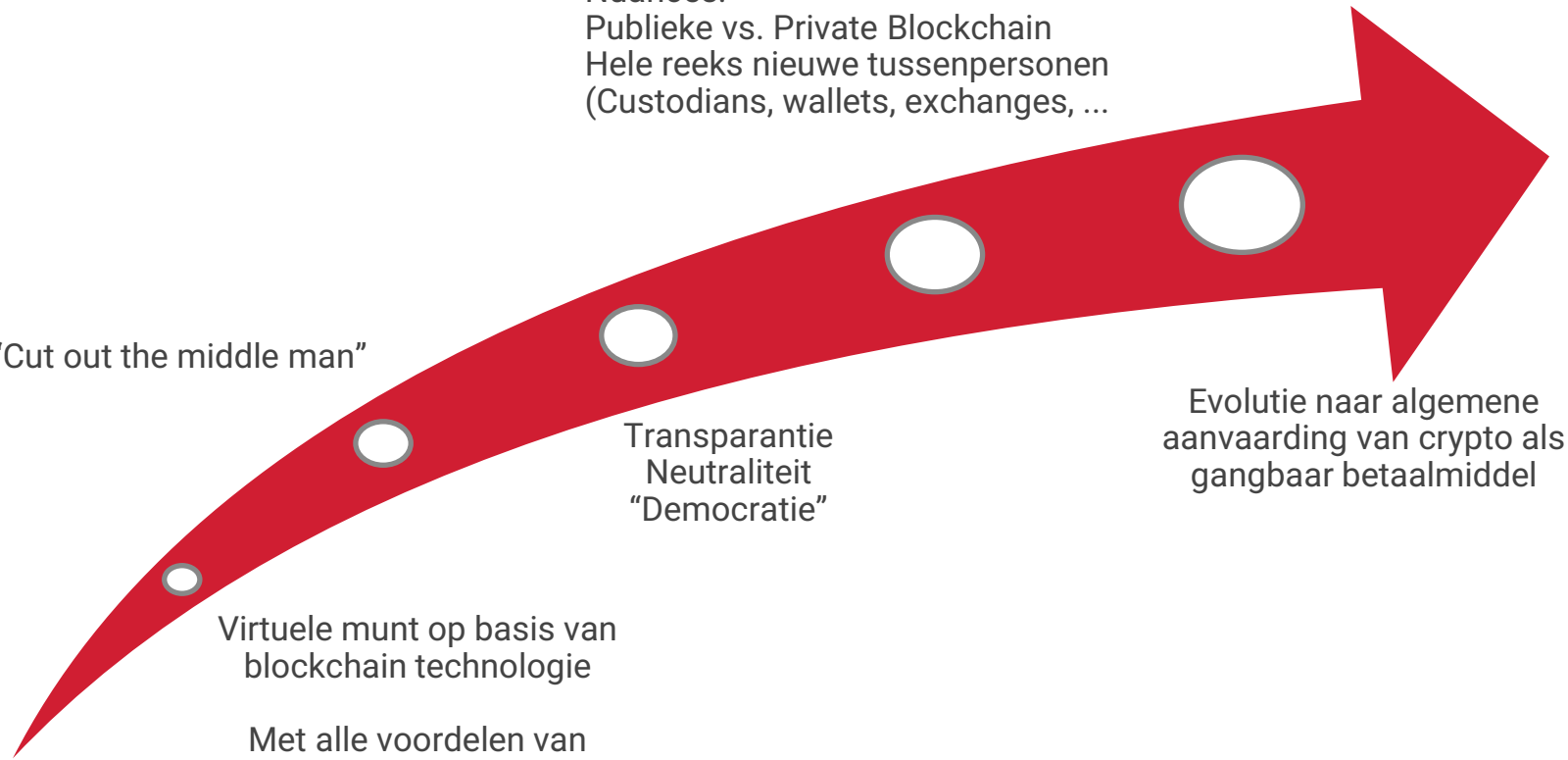


2008
Bitcoin whitepaper

2017
De zeepbel barst (een eerste keer)

2021 - 2022
Zeepbel barst een tweede keer
Nieuwe zeepbel: NFT's...?

Nuances:
Publieke vs. Private Blockchain
Hele reeks nieuwe tussenpersonen
(Custodians, wallets, exchanges, ...



“Cut out the middle man”

Virtuele munt op basis van blockchain technologie

Met alle voordelen van Blockchain technologie

Transparantie
Neutraliteit
“Democratie”

Evolutie naar algemene aanvaarding van crypto als gangbaar betaalmiddel

Basics

"Mining"

Aankoop/verkoop (exchange)

"Tokenisatie"

"Fungible tokens" (onderling inwisselbaar, zoals geld)

Risicoanalyse

Beperkte aanvaarding en vertrouwen (basis van elke munt)

Perfect voor misdaadmilieu

Erg volatiel

ICO

Probleem:
Nauwelijks of geen Wetgeving
Juridische onzekerheid
Behalve in CH, Malta en enkele andere landen

ICO

"Initial Coin Offering"
Uitgifte van "tokens" tegen betaling
Cfr IPO, uitgifte aandelen
Populaire manier om fondsen in te zamelen voor cryptoprojecten

“Virtueel geld is elke vorm van **niet gereglementeerd digitaal geld zonder wettelijke betaalkracht**”

Reglement 3 april 2014 van de Autoriteit voor Financiële Diensten en Markten betreffende het commercialiseringsverbod van bepaalde financiële producten aan niet-professionele cliënten

Enige Belgische wetgeving

Té ruime definitie (omvat ook niet-cryptomunten) enerzijds en té enge definitie anderzijds (omvat niet alle cryptoactiva)

“een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld”

AMLD5

Beperkt toepassingsgebied

Viseert uitwisselingsplatformen en bepaalde soorten wallets

Veel spelers vallen niet onder het vangnet

“een digitale weergave van waarde of rechten die elektronisch kan worden overgedragen en opgeslagen, met gebruikmaking van Distributed Ledger Technology of vergelijkbare technologie”

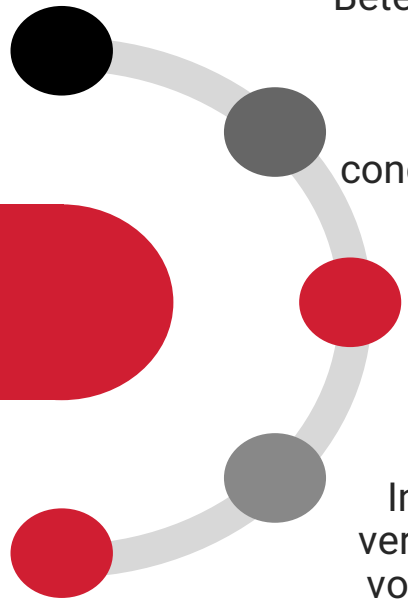
Voorstel van verordening betreffende markten in cryptoactiva (MiCA)

MiCA Verordening

(Markets in Crypto-assets)

Eerste ontwerp van Europees regelgevend kader voor cryptocurrencies

Timing: wellicht 2023, met 18 maanden overgangsperiode



Duidelijkheid en rechtszekerheid
Betere bescherming voor consument en investeerder
Betere concurrentiepositie voor EU

Geïnspireerd op klassieke financiële diensten

Invoering van een vergunningssysteem voor cryptodiensten

Invoering van gedragsregels en consumentenbescherming

1. Uitgevers betrokken bij ICO's moeten vergunning hebben.
MiCA onderscheid 3 soorten uitgevers
"Asset referenced tokens", "e-money tokens", "andere" tokens
Enkel die laatste zijn vrijgesteld van vergunningsplicht

2. "Vergunning is onderworpen aan voorwaarden
Voldoende dekking aanhouden
Prospectusplicht (maar geen voorafgaande goedkeuring)
EMD II (Electronic Money Directive II)

3. Aanbieders van andere diensten moeten meestal ook een vergunning bekomen
8 soorten diensten, waaronder crypto exchanges, wisselkantoren, brokers, adviesverleners, wallets, ...

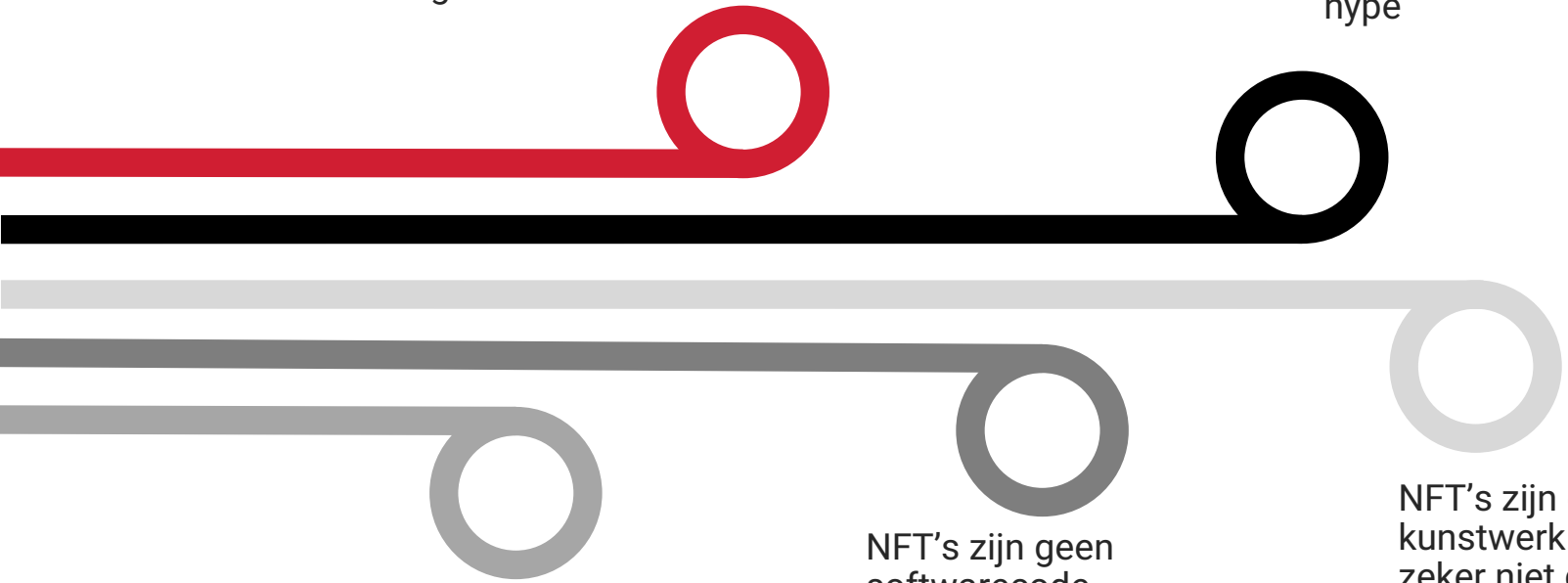
4. Bestaande kredietinstellingen moeten geen nieuwe vergunning bekomen. Dat geldt ook voor beleggingsondernemingen onder MiFID (tenminste als cryptodienst gerelateerd is aan klassieke beleggingsdienst)

5. Publiek aanbod van crypto is vrijgesteld van vergunningsplicht als aan een reeks voorwaarden voldaan is
O.m. crypto is gratis, niet inwisselbaar, aanbod beperkt tot 150 personen per lidstaat, tot waarde max 1 mio euro, ...

NFT’s
Non fungible tokens

Van maart 2021: 70 mio USD voor “het eerste digitale kunstwerk in NFT” (Everydays; the first 5000 days)
Over 2,9 mio voor “de eerste tweet”
Tot in november 2021: Wout Van Aert “veilt” 4 van zijn “overwinningen” in NFT...

“Non fungible tokens” zijn duidelijk een nieuwe (dure) hype



NFT’s zijn geen tastbaar kunstwerk. NFT’s zijn al zeker niet de echte overwinningen van Wout Van Aert...

NFT’s zijn geen softwarecode

Maar wat zijn ze dan wel…?
De volgende zeepbel?
Of…?

Wat we wel weten...

Non fungible token	**Niet inwisselbaar, maar wel verhandelbaar. Waarde = de waarde die de koper wil geven…**
Bevestigt “originaliteit” van (digitaal) voorwerp	**Creëert valse schaarste en creëert collector’s items “Pokémon goes digital”...**
Echtheid gegarandeerd via blockchain	**Digitaal voorwerp wordt “beschreven” in metadata en die data wordt, samen met eigendomsdata en “echtheidsgarantie weggeschreven in blockchain**
“Uniek digitaal actief”	**Blockchain certificaat “garandeert” echtheid van digitaal (of fysiek) voorwerp of gebeurtenis (concert, internet meme, eerste tweet, …)**
Aankoop/verkoop vaak via Smart Contracts	**Gespecialiseerde beursplatformen schieten als paddestoelen uit de grond**

Waarom het toch vooral ook als een zeepbel aanvoelt

“Eigendomsrecht”

Je bent géén eigenaar
Geen bezitsrecht
Geen rustig genot
Zeker geen IP-rechten

Continuïteit en ToU

Wat als platform verdwijnt?
Wat met corrupte code?

Wat met “namaak” van “origineel” object (al dan niet door artiest zelf)?

GDPR (eens te meer)

Consumenten-bescherming

Piramideverkoop / Ponzi
WER-verplichtingen

Fraude
Witwassen
(Zwart) geld verplaatsing
Drugs- en mensenhandel
Belastingontduiking
...

Geen specifieke wetgeving

Maar tal van juridische vragen...

“Volgrecht” voor de creator

Op basis van smart contract code

Namaakbestrijding Auteursrecht, merkenrecht, modellen

NFT als echtheidscertificaat

Waarde creëren voor artiesten / creators

Maar opgepast voor de zeepbel / oneerlijke marktpraktijken

Nieuwe markt voor collectables en gaming

Koppeling aan fysieke objecten

Wordt eigendomsbewijs op bvb kunstwerk (cfr Nike)

Required action by data importer (Inform, waive, minimize, …)
Cfr new SCC’s

Opportuniteiten?