Jaarlijksessie van de subwerkgroep inzake informatieveiligheid van het netwerk DB2P

Juni 2023

pensionpro

sigedis

Mery Nange

Functionaris voor de gegevensbescherming Sigedis

pensionpro

sigedis

1. Inleiding

- Onthaal
- Inhoud van de sessie
- Het secundaire netwerk en zijn leden

2. Top drie niet-conforme normen

- Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support
- Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : design, implementatie en testen
- Organisatie van de informatieveiligheid
- Medewerkers-gerelateerde veiligheid

3. Varia

- NIS II Evolutie
- New rules of the Data Governance Act - 24 September 2023
- Vragenlijst 2023 van de minimale veiligheidsnormen en contactgegevens voor DPO/contacts
- Andere

sigedis

1. Inleiding

Onthaal

- Dankwoorden
- Praktische informatie

Inhoud van de sessie

- Inleiding
- 3 Top drie niet-conforme normen binnen het netwerk
- Varia

* IP : institution de pension / OP : Organisme de Pensions

1. Inleiding

Het secundaire netwerk en zijn leden

Een kleine herinnering :

Waarom deze jaarlijkse sessie van de subwerkgroep “information security ” van het netwerk db2p ?

In overeenstemming met de norm 5.3.1.4 Secundair netwerk « Elke organisatie van een secundair netwerk moet minstens één keer per semester relevante informatie uitwisselen met haar secundair netwerk door een vergadering van de subwerkgroep "Informatieveiligheid" te organiseren voor de organisaties die deel uitmaken van haar netwerk »

De leden ?

Het netwerk Db2p (Database van de tweede pilier) telt momenteel : 203 leden
Dit is de specifieke sector van de aanvullende pensioenen binnen het socialezekerheid waarvan het beheer wordt gezamenlijk waargenomen door een openbare instelling van sociale zekerheid, de KSZ en private instanties, de “meewerkende instellingen van sociale zekerheid”, Sigedis.
Meer info: Tweede pensioenpijler | Kruispuntbank van de Sociale Zekerheid (fgov.be) en https://pensionpro.be/

Informatie voor pensioeninstellingen ?

Nieuwe website van de KSZ : 01/06/2023 –
Ref: https://ksz-bcss.fgov.be/nl/over-de-ksz/structuur-van-het-netwerk

1. Inleiding

Ter herinnering: de basisregels….

DPO

- Ten minste 1 DPO per organisatie
- Notificatie van de DPO aan de KSZ (security@ksz-bcss.fgov.be) en Sigedis (dpo-db2p@sigedis.fgov.be) die bekend moeten zijn bij de GBA (De Gegevensbeschermingsautoriteit):
  - ✓ Om aan te sluiten bij het netwerk Db2p;
  - ✓ Telkens wanneer de DPO wijzigt.

Vragenlijst

- 1/jaar;
- Terug te bzoegzn vóór 1 oktober 2023;
- De vragenlijst is beschikbaar op de website van KSZ en Sigedis

Deelname aan de sessie

- Verplicht
- Twee sessie in NL en FR.

* IP : institution de pension / OP : Organisme de Pensions

Ivan Verstraeten

Veiligheidsconsulent

KSZ

pensionpro

sigedis

2. Top 3 niet-conforme normen van het Db2P-netwerk

De analyse van de vragenlijsten voor 2022 heeft het mogelijk gemaakt om een top 3 van minimumnormen samenstellen waarbij men moeilijkheden heeft om ze correct na te leven:

Oorzaken?

- Moeilijk te begrijpen normen;
- Normen die worden beheerd op het niveau van de serviceprovider;
- Afwezigheid van DPO's of opgeleid personeel.

Wat is de Top 3?

- ❑ Normen 5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen):
  - ➢ transition en ICT support;
  - ➢ design, implementatie en testen.
- ❑ Norme 5.3. Organisatie van de informatieveiligheid.
- ❑ Norme 5.4. Veiligheid gerelateerd aan medewerkers.

sigedis

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

De norm is bedoeld voor:

- 5.9.2 Het beheer van de in productiestelling
- 5.9.5 Het loggen van de toegang

en

- 5.11.12 Inventaris
- 5.11.7e Logbeheer tijdens een project

Hoe hieraan te voldoen?

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

Norm 5.9.2: Het beheer van de in productiestelling

- Beschikken over procedures (document) voor:
  - de in productiestelling van nieuwe toepassingen;
  - Het aanbrengen van aanpassingen aan bestaande toepassingen.

- Vermijd dat één en dezelfde persoon zorgt voor controle over dit hele proces (controle).

Meer details over de te nemen maatregelen:
Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties.
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. et 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

Norm 5.9.5 Het loggen van de toegangen

- Uitwerken van een logboekprocedure (Document);

- Definieren van gestructureerde logboeken (bestanden) voor:
  - Transacties
  - Controlewerkzaamheden,
  - Gebruikersactiviteiten (toepassingslogboeken),
  - Uitzonderingen

sigedis

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

Gebeurtenissen met betrekking tot informatiebeveiliging en privacy (privacylog)

- Zorg voor logboekregistratie aan het begin van het ontwerp – By Design (controle);
- Betreft alle toegangen tot sociale of medische gegevens (controle);
- Interne kloksynchronisatie (besturing);
- Opzetten of ontwikkelen van tools voor consultatie (Applicatie);
- Het gebruik van de tools en het systeem moet worden gelogd (bestanden).

Meer details over de te nemen maatregelen?

- Richtlijn informatiebeveiliging en privacy - Log Management (BLD_Gestion logs)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

Norm 5.11.12 Inventaris.

- Toevoegen van alle assets, inclusief verworven of ontwikkelde systemen aan het operationele asset management systeem (bestand)

Meer details over de te nemen maatregelen?
Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en 5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van ICT informatiesystemen (toepassingen) : transition en ICT support

Norm 5.11.7e Logbeheer tijdens een project.

- Bewaren van loggegevens:
  - functioneel/transactioneel bewaard gedurende ten minste 10 jaar;
  - technisch/infrastructureel gedurende minstens 2 jaar.

Meer details over de te nemen maatregelen?

Richtlijn informatiebeveiliging en privacy
Log Management (BLD_Gestion logs)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11: Aanschaf, ontwerp, ontwikkeling en onderhoud van ICT-informatiesystemen (toepassingen): ontwerp, implementatie en testen

De norm is bedoeld om te voldoen aan:

- 5.9.1 Scheiding van omgevingen
- *5.9.5 Logging toegang*
- 5.9.6 Traceerbaarheid van de identiteiten.
- 5.11.2 Toegangsbeheer
- 5.11.5. Controle voor in productie stelling
- 5.11.7b1 Logbeheer tijdens een Project
- 5.11.9 Continuïteitsbeheer tijdens een project
- 5.11.10 Incidentenbeheer tijdens een project
- *5.11.12 Inventaris.*

Hoe hieraan te voldoen?

Norm 5.9.1

- Elke ontwikkeling of test is verboden in de productie-omgeving (controle).

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9 Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen implementatie en testen

Norm 5.9.6 Traceerbaarheid van de identiteiten.

- Zorg voor de traceerbaarheid van identifiers die intern door de organisatie worden gebruikt (control).

Meer details over de te nemen maatregelen?

Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen, implementatie en testen

Norm 5.11.2 Toegangsbeheer

- Hou rekening met bestaande toegangsbeheersystemen;
- Definiëren, documenteren, valideren en communiceren van toegangsbeveiligingsvoorwaarden;
- Vermijd toegangsbeheer in een toepassing waar formele procedures zijn om alle fasen van de levenscyclus van toegangsbeveiliging te beheren;
- Wanneer een programma wordt ontwikkeld en een programmanummer wordt gebruikt om zich te identificeren binnen het sociale zekerheidsnetwerk, moet de organisatie dit programmanummer kunnen koppelen aan de identiteit van de natuurlijke persoon binnen de organisatie die dit bericht verzendt.

Meer details over de te nemen maatregelen?
Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen, implementatie en testen

Norm 5.11.5 Controle voor in productie stelling.

- ervoor te zorgen dat de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden (controle).
  - ❑ Definieer beveiligings- en privacymaatregelen aan het begin van het project;
  - ❑ Controle tijdens de productie.

Meer details over de te nemen maatregelen?

Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen, implementatie en testen

Norm 5.11.7b1 Logbeheer tijdens de looptijd van een project

Verduidelijken, in de specificaties van het project:

- Hoe de toegang tot en het gebruik van systemen en applicaties worden vastgelegd (Document).

- Doelstellingen:
  a) snel, eenvoudig en duidelijk kunnen vaststellen wie toegang heeft gekregen tot welke informatie
  b) Wanneer
  c) en hoe

Meer details over de te nemen maatregelen?
Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen, implementatie en testen

Norm 5.11.9 Continuïteitsbeheer tijdens een project

- Formaliseer behoeften met betrekking tot de continuïteit van de dienstverlening;
- Integreer duidelijk in de programma's, de herstelpunten die moeten worden gedefinieerd om operationele problemen aan te pakken (document: Operationeel bestand);
- Specifieke maatregelen voor een back-up en herstel ("herstel") van informatie (controle);
- Hou rekening met de vereisten van de organisatie voor probleemtolerantie en infrastructuurredundantie (controle);
- Het continuïteitsplan en de procedures bijwerken in functie van de evolutie van het project;
- Voer aan het begin van het project een risicoanalyse uit om noodprocedures te definiëren

Meer details over de te nemen maatregelen?
Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

sigedis

2. Top 3 niet-conforme normen van het Db2P-netwerk

5.9. Operationeel beheer en .11 : Aankoop, ontwerpeb, ontwikkelen en onderhouden van ICT-informatiesystemen (applicaties): ontwerpen, implementatie en testen

Norm 5.11.10 Incidentenbeheer tijdens een project

- Tijdens de ontwikkeling van een project (Document)
  - ❑ Formaliseer incident management procedures;
  - ❑ Valideer procedures voor incidentbeheer.

- De Security Advisor (DPO) moet tijdens de ontwikkeling van een project op de hoogte worden gebracht van beveiligings- en privacyincidenten

Meer details over de te nemen maatregelen?

Richtlijnen voor informatiebeveiliging en privacy Aankoop, ontwerp, ontwikkeling en onderhoud van applicaties
Bld_appdev_projet - (BLD APPDEV)

2. Beveiligingsregels binnen het DB2P-netwerk

5.3. Organisatie van de informatieveiligheid

De norm is bedoeld om aan de volgende doelstellingen te voldoen :

- 5.3.1.1 Personeelsgerelateerde aspecten
- 5.3.1.2 Organisatie van informatieveiligheid
- 5.3.1.3 Beslissingsplatform
- 5.3.1.4 Secundair netwerk
- 5.3.1.5 Informatieveiligheid in het kader van projecten

Hoe te voldoen ?

Norm 5.3.1.1 Personeelsgerelateerde aspecten

- Vóórr ondertekening van het contract (checklist) :
  - De profiel nagaan van kandidaten voor functies die een belangrijk risico vormen voor informatieveiligheid;
  - Verantwoordelijkheden van de partijen ten aanzien van informatieveiligheid en privacy moeten vastgelegd zijn.

2. Beveiligingsregels binnen het DB2P-netwerk

5.3. Organisatie van de informatieveiligheid

- Tijdens de looptijd van het contract:

  De werknemers:
  - Zijn verplicht om informatiebeveiliging en privacy toe te passen;
  - Moeten geschikte training en regelmatige bijscholing krijgen met betrekking tot minimale normen en procedures van de organisatie.

  De organisatie moet:
  - Regelmatig verifiëren van het profiel van medewerkers met veiligheidsgevoelige functies;
  - een formeel disciplinair proces voorzien voor medewerkers die een inbreuk op informatieveiligheid of privacy hebben gepleegd;
- Beëindiging of wijziging van dienstverband :
  - Bepalen en communiceren van de verantwoordelijkheden en verplichtingen rond informatieveiligheid en privacy.

sigedis

2. Beveiligingsregels binnen het DB2P-netwerk

5.3. Organisatie van de informatieveiligheid

Norm 5.3.1.2 Interne organisatie van de informatieveiligheid (document)

- Informatieveiligheidsdienst die wordt geleid door een veiligheidsconsulent (CISO/DPO)/ Erkende Gespecialiseerde informatieVeiligheidsDienst (EGVD);
- De identiteit van haar CISO(DPO) en zijn eventuele adjuncten meedelen aan KSZ/Sigedis;
- In het bezit zijn van een veiligheidsplan;
- Over de nodige werkingskredieten beschikken;
- Aan de KSZ het aantal uren meedelen;
- Een periodieke communicatie i.s.m. de veiligheidsconsulent organiseren;

2. Beveiligingsregels binnen het DB2P-netwerk

5.3. Organisatie van de informatieveiligheid

Norm 5.3.1.3 Beslissingsplatform (verslag)

- Een beslissingsplatform opzetten om:
  - informatiebeveiligings- en privacy-maatregelen te valideren;
  - het goedkeuren van informatiebeveiligings- en privacy-maatregelen.

2. Beveiligingsregels binnen het DB2P-netwerk

5.3. Organisatie van de informatieveiligheid

Norm 5.3.1.5 Informatieveiligheid in het kader van projecten

- beschikken over procedures voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de informatieveiligheid- en privacy-vereisten die in dit document beschreven worden

2. Beveiligingsregels binnen het DB2P-netwerk

5.4. Medewerkers-gerelateerde veiligheid

De norm is bedoeld om:

- 5.4.1 Rapportage-, evaluatie- en bewustmakingscampagn;
- 5.4.2 Toegang tot informatie.

Hoe hieraan te voldoen ?

Norm 5.4.1 Rapportage-, evaluatie- en bewustmakingscampagne

- Minstens 1/jaar, een sensibiliseringscampagne of informatiesessie organiseren met betrekking tot informatiebeveiliging en privacy om:
  - De informatieveiligeheid en de privacy te valideren
  - Hierover te communiceren
  - Een een opvolging te verzekeren
- Voer jaarlijks een beoordeling uit over de naleving van dit beleid in de praktijk (d,m,v, een interne enquête).

sigedis

2. Beveiligingsregels binnen het DB2P-netwerk

5.4. Medewerkers-gerelateerde veiligheid

Norm 5.4.2 Toegang tot informatie

- Ontwikkel een beleidslijn waarin gesteld wordt dat de samenwerking van alle medewerkers essentieel is voor informatiebeveiliging en privacy. Elke medewerker speelt een cruciale rol in het voorkomen van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegang tot informatiesystemen en -toepassingen als voor de fysieke toegang tot gebouwen of documenten.
- Ontwikkel een richtlijn waarin staat dat de gebruiker verantwoordelijk blijft voor de informatie, ongeacht de vorm waarin deze informatie wordt vastgelegd. De gebruiker dient dus te zorgen voor een goede bescherming hiervan. Zodra de informatie niet langer door de gebruiker wordt gebruikt, moet deze er ook voor zorgen dat deze wordt gearchiveerd of vernietigd.
- Implementeer een toegangssysteem (fysiek of logisch) om ongeautoriseerde toegang tot de organisatie te voorkomen. De toegang wordt beveiligd door nauwkeurige toestellen voor toegangscontrole

sigedis

Directive Nis-II

v

Minimale Normen van het netwerk van de socia
zekerheid

3. Varia - NIS II (Network and Information Systems)

16 Januari 2023

➢ NIS II - Directive (EU) 2022/2555 : Toepassingsgebied en aanduiding entiteiten : Evolutie

Doel NIS-2

Betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie

CENTRE FOR CYBER SECURITY BELGIUM

Cyberfundamentals framework

Versterking van de risicobeheersmaatregelen op het gebied van cyberbeveiliging

Deze maatregelen zijn gebaseerd op een benadering “all risks’ en die tot doel heeft om netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen

Toepassingsgebied

Kritische sectoren

Essentiële en belangrijke entiteiten

Andere kritieke sectoren

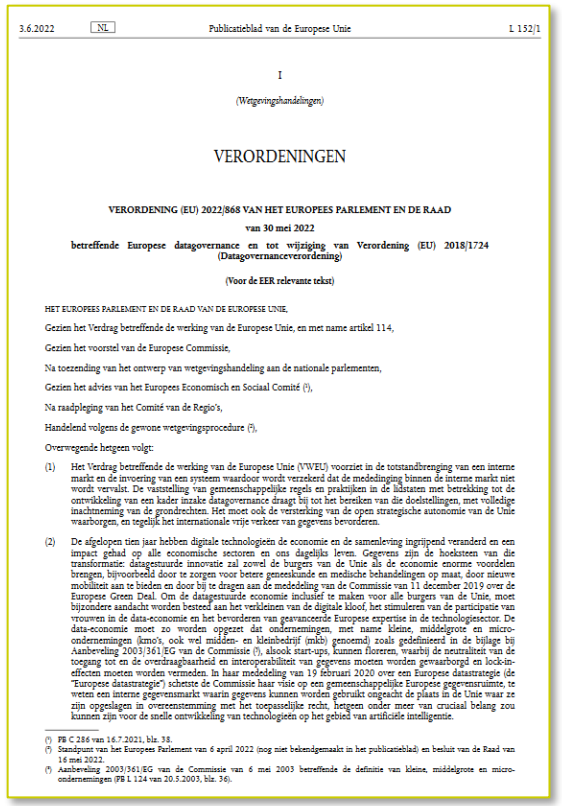
Belangrijke entiteiten

17 October 2024

sigedis

3. Varia – Data Governance Act

- New rules of the Data Governance Act - REGULATION 2022/86824 of 30 May 2022
- Inwerkingtreding **24 September 2023**



3.6.2022 NL Publicatieblad van de Europese Unie L 152/1

I

(Wetgevingshandelingen)

VERORDENINGEN

VERORDENING (EU) 2022/868 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 30 mei 2022

betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité (1),

Na raadpleging van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure (2),

Overwegende hetgeen volgt:

(1) Het Verdrag betreffende de werking van de Europese Unie (VWEU) voorziet in de totstandbrenging van een interne markt en de invoering van een systeem waardoor wordt verzekerd dat de mededinging binnen de interne markt niet wordt vervalst. De vaststelling van gemeenschappelijke regels en praktijken in de lidstaten met betrekking tot de ontwikkeling van een kader inzake datagovernance draagt bij tot het bereiken van die doelstellingen, met volledige inachtneming van de grondrechten. Het moet ook de versterking van de open strategische autonomie van de Unie waarborgen, en tegelijk het internationale vrije verkeer van gegevens bevorderen.

(2) De afgelopen tien jaar hebben digitale technologieën de economie en de samenleving ingrijpend veranderd en een impact gehad op alle economische sectoren en ons dagelijks leven. Gegevens zijn de hoeksteen van die transformatie: datagestuurde innovatie zal zowel de burgers van de Unie als de economie enorme voordelen brengen, bijvoorbeeld door te zorgen voor betere geneeskunde en medische behandelingen op maat, door nieuwe mobiliteit aan te bieden en door bij te dragen aan de mededeling van de Commissie van 11 december 2019 over de Europese Green Deal. Om de datagestuurde economie inclusief te maken voor alle burgers van de Unie, moet bijzondere aandacht worden besteed aan het verkleinen van de digitale kloof, het stimuleren van de participatie van vrouwen in de data-economie en het bevorderen van geavanceerde Europese expertise in de technologiesector. De data-economie moet zo worden opgezet dat ondernemingen, met name kleine, middelgrote en micro-ondernemingen (kmo's, ook wel midden- en kleinbedrijf (mkb) genoemd) zoals gedefinieerd in de bijlage bij Aanbeveling 2003/361/EG van de Commissie (3), alsook start-ups, kunnen floreren, waarbij de neutraliteit van de toegang tot en de overdraagbaarheid en interoperabiliteit van gegevens moeten worden gewaarborgd en lock-in-effecten moeten worden vermeden. In haar mededeling van 19 februari 2020 over een Europese datastrategie (de "Europese datastrategie") schetste de Commissie haar visie op een gemeenschappelijke Europese gegevensruimte, te weten een interne gegevensmarkt waarin gegevens kunnen worden gebruikt ongeacht de plaats in de Unie waar ze zijn opgeslagen in overeenstemming met het toepasselijke recht, hetgeen onder meer van cruciaal belang zou kunnen zijn voor de snelle ontwikkeling van technologieën op het gebied van artificiële intelligentie.

(1) PB C 286 van 16.7.2021, blz. 38.
(2) Standpunt van het Europees Parlement van 6 april 2022 (nog niet bekendgemaakt in het publicatieblad) en besluit van de Raad van 16 mei 2022.
(3) Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

Doel:

- Faciliteren van het hergebruik van data, beheerd door openbare instellingen
- Toegang tot data verbeteren
- Veilige *Data sharing* aanmoedingen

Data houder ↔ Data bemiddelaar ↔ Data gebruiker

Bv. pensioendienst

Commerciële relatie & vergoeding

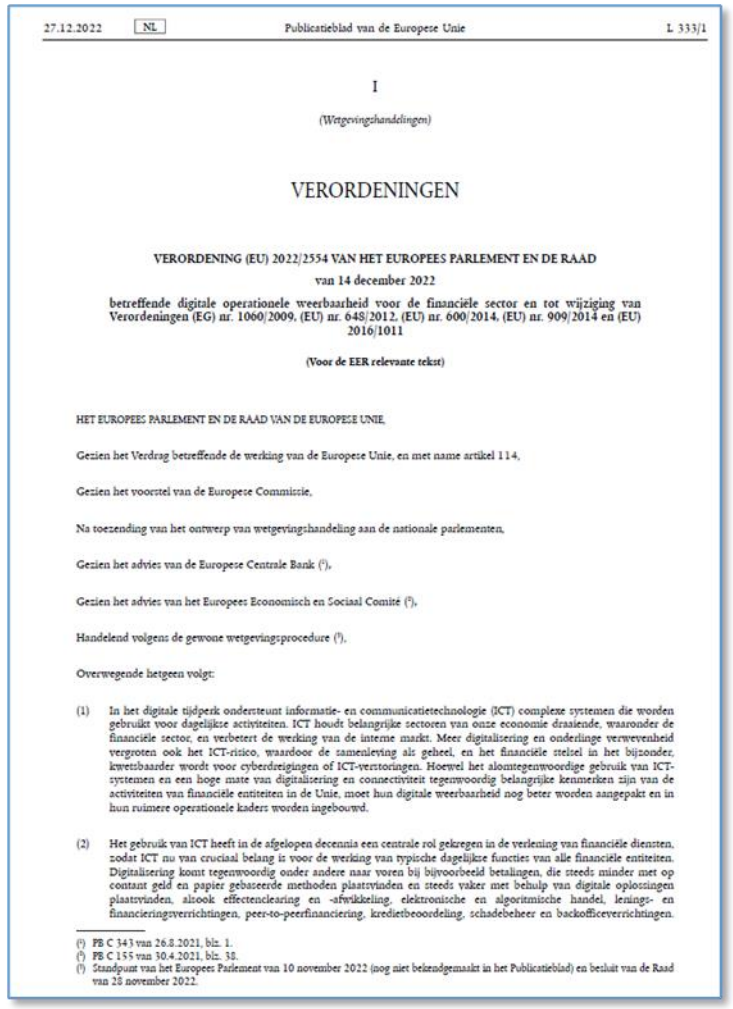
Bv. FinTech Co X maakt een App

Maatregelen:

- Verbod op exclusieve overeenkomsten voor data re-use tussen openbare instellingen
- Verplichting om persoonsgegevens te anonimiseren, en te beveiligen
- Gelijke voorwaarden voor data sharing & non-discriminatie

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022R0868

4. Digital Operational Resilience Act (DORA)



27.12.2022 NL Publicatieblad van de Europese Unie L 333/1

I

(Wetgevingshandelingen)

VERORDENINGEN

VERORDENING (EU) 2022/2554 VAN HET EUROPEES PARLEMENT EN DE RAAD
van 14 december 2022
betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van de Europese Centrale Bank (1),

Gezien het advies van het Europees Economisch en Sociaal Comité (2),

Handelend volgens de gewone wetgevingsprocedure (3),

Overwegende hetgeen volgt:

(1) In het digitale tijdperk ondersteunt informatie- en communicatietechnologie (ICT) complexe systemen die worden gebruikt voor dagelijkse activiteiten. ICT houdt belangrijke sectoren van onze economie draaiende, waaronder de financiële sector, en verbetert de werking van de interne markt. Meer digitalisering en onderlinge verwevenheid vergroten ook het ICT-risico, waardoor de samenleving als geheel, en het financiële stelsel in het bijzonder, kwetsbaarder wordt voor cyberdreigingen of ICT-verstoringen. Hoewel het alomtegenwoordige gebruik van ICT-systemen en een hoge mate van digitalisering en connectiviteit tegenwoordig belangrijke kenmerken zijn van de activiteiten van financiële entiteiten in de Unie, moet hun digitale weerbaarheid nog beter worden aangepakt en in hun ruimere operationele kaders worden ingebouwd.

(2) Het gebruik van ICT heeft in de afgelopen decennia een centrale rol gekregen in de verlening van financiële diensten, zodat ICT nu van cruciaal belang is voor de werking van typische dagelijkse functies van alle financiële entiteiten. Digitalisering komt tegenwoordig onder andere naar voren bij bijvoorbeeld betalingen, die steeds minder met op contant geld en papier gebaseerde methoden plaatsvinden en steeds vaker met behulp van digitale oplossingen plaatsvinden, alsook effectenclearing en -afwikkeling, elektronische en algoritmische handel, leenings- en financieringsverrichtingen, peer-to-peerfinanciering, kredietbeoordeling, schadebeheer en backofficeverrichtingen.

(1) PB C 343 van 26.8.2021, blz. 1.
(2) PB C 155 van 30.4.2021, blz. 38.
(3) Standpunt van het Europees Parlement van 10 november 2022 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 28 november 2022.

- EU-Verordening 2022/2554 van 14 December 2022
- **Doel** - versterken weerbaarheid tegen calamiteiten op het vlak van IT operations van banken, verzekeringinstellingen en beleggingsondernemingen
- **Doelgroep -** de financiële sector - entiteiten die financiële diensten aanbieden zoals banken, verzekeringsinstellingen en beleggingsondernemingen
- **MNM, NIS2 en DORA** - Ten opzichte van NIS2 is DORA een specifieke regelgeving voor een gerichte doelgroep.

  Gelet op het specifieke personeel toepassingsgebied van DORA zijn er geen plannen om de minimale normen (MNM) aan te passen aan de verplichtingen die volgen uit DORA

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022R0868

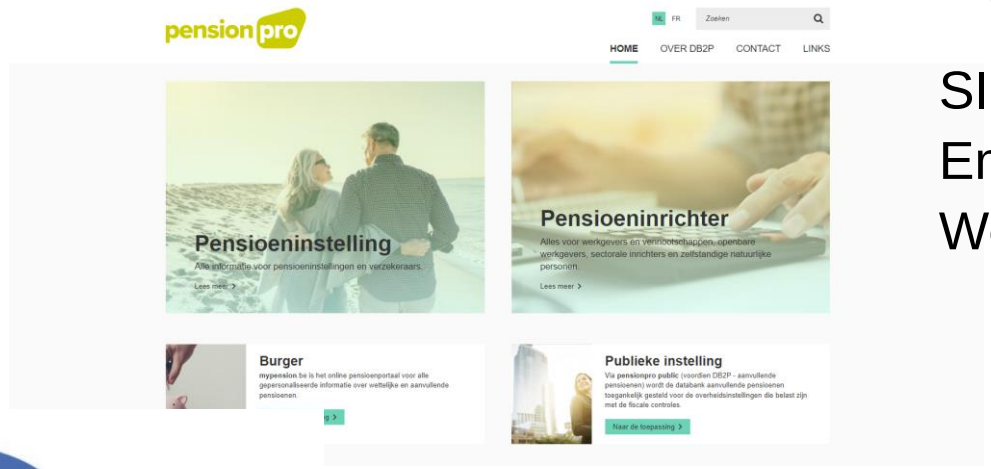
3. Varia – Vragenlijst / DPO & contacten

Vragenlijst minimumnormen 2022-2023 en contactgegevens van DPO's en contactpersonen

- Vragenlijst 2022-2023 uiterlijk tegen 1 oktober 2023 in te dienen.
  - Het document is beschikbaar op de website van ksz-bcss.fgov.be en pensiopro.be
  - Retourneer de ondertekende vragenlijst (in Excel, indien ondertekend in pdf, retourneer dan de Excel)
  - Naar de BCSS en Sigedis
- Aan Sigedis mee te delen gegevens
  - Identiteit en contactgegevens van de DPO en eventuele plaatsvervangers
  - Coördinaten van een contactpersoon voor de organisatie

Bedankt voor uw aandacht !

Merci pour votre attention !



SIGEDIS : Service sécurité / Veiligheidsdienst
Email : dpo-db2p@sigedis.fgov.be
Website : https://pensionpro.be/

KSZ – BCSS : Service sécurité / Veiligheidsdienst
Email : security@ksz-bcss.fgov.be
Website: https://www.ksz-bcss.fgov.be