Federal Information Security Policy Guideline

Handleiding voor de beveiliging van persoonsgegevens

21/11/2019

FISPDOC07 V2.1

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen worden beschouwd als adviezen die redelijkerwijs op een gemeenschappelijke manier van toepassing zijn op alle federale diensten. Deze zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

FISP Werkgroep

.be

INHOUDSTAFEL

Inhoud van dit document

Oriëntatie van het document

Dit document maakt integraal deel uit van methodologie voor informatiebeveiliging binnen de Federale overheid (FISP-project).

Veiligheidsdoel van het document

Dit document omschrijft de vereisten om te voldoen aan de informatiebeveiliging zoals vooropgesteld door de Algemene Verordening Gegevensbescherming (AVG). Het bevat bovendien een gestandaardiseerde categorisatie volgens de interpretatie van FISP werkgroep.

Toepassingsgebied

Deze handleiding voor privacy en beveiliging is van toepassing op alle persoonlijke informatie die door de federale overheid (en haar dienstverleners) wordt verwerkt.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Deze informatie mag niet individueel gebruikt worden als referentie documentatie. De lezer van dit document gebruikt dit document niet als vervanger van de wetgeving, maar als leidraad bij nemen van de gepaste beveiligingsmaatregen en de evaluatie van de categorieën van persoonsgegevens.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (FGB of ook wel DPO) van de openbare instelling van federale overheid, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen) en andere belanghebbenden in verwante gebieden (bv. de documentenbeheerder).

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Het toenemende gebruik en de waarde van persoonlijke informatie, het delen van persoonlijke informatie tussen diensten en de toenemende complexiteit van ICT-systemen kunnen het voor een organisatie moeilijk maken om gegevensbescherming te waarborgen en de naleving van de verschillende toepasselijke wetten te bereiken. Belanghebbenden op het gebied van gegevensbescherming kunnen onzekerheid en wantrouwen voorkomen door goed om te gaan met kwesties en gevallen van misbruik van persoonlijke informatie te voorkomen.

Om verwarring te vermijden gebruiken we "**gegevensbescherming**" **(of "dataprotectie")** om te verwijzen naar de bescherming en het beheer van **persoonlijke data** zoals beschreven in de **AVG**.

Als we "**informatiebeveiliging**" gebruiken, zijn dat meer algemene maatregelen die betrekking hebben op beveiliging van **bedrijfsgegevens** onder BSG en ISO27001.

Dus de bescherming van persoonsgegevens overlapt gedeeltelijk met informatiebeheer en informatiebeveiliging, en heeft een nieuwe dimensie gekregen door de publicatie en de inwerkingtreding van de AVG van de Europese Raad en het Parlement. Een overheid is onderworpen aan de regels van de AVG wanneer zij persoonsgegevens verwerkt.

Informatiebeveiliging (en ook databescherming) is gebaseerd op 3 pijlers die op mekaar moeten afgestemd zijn: "PPT" of "Personen, Processen en Technologie". Het is essentieel dat elk van deze 3 activiteiten in evenwicht worden gehouden om voldoende beveiliging te kunnen garanderen.

Dit document omvat slechts een summiere samenvatting van vereisten om te voldoen aan gegevensbescherming zoals vooropgesteld door de AVG. Het is niet het doel van dit document om uw organisatie in overeenstemming te brengen met de AVG. Dit document geeft geen interpretatie weer van de AVG maar biedt enkel praktische beveiligingsmaatregelen aan om gegevensbescherming te garanderen. Het bevat bovendien een gestandaardiseerde categorisatie bepaald door de FISP Werkgroep. Al de niet-besproken principes van de AVG blijven ook van toepassing net zoals alle andere wetten, regelgevingen en globale beveiligingsmaatregelen die van toepassing zijn op uw federale organisatie.

Wettelijk Kader

Organisaties zijn om verschillende redenen verplicht om persoonlijke gegevens te beschermen: om de gegevensbescherming van personen te beschermen, om te voldoen aan wettelijke en reglementaire vereisten, om bedrijfsverantwoordelijkheid uit te oefenen, om het vertrouwen van de consument te vergroten, enz.

Algemene Verordening Gegevensbescherming (AVG)

Er zijn verschillende wettelijke verplichtingen om gegevens bescherming te garanderen. De federale organisaties dienen dan ook te handelen met respect voor de specifieke wetten die op hun organisatie van toepassing is. Recent is de algemene verordening gegevensbescherming van het Europees Parlement en de Raad, die op 27 april 2016 werd goedgekeurd, op 25 mei 2018 in werking getreden (AVG).[1] Daarnaast is er ook de Belgische federale wet van 30 juli 2018 waarin de Belgische overheid getracht heeft om ook hun eigen regelgeving aan te passen.

Het belangrijkste idee naast deze nieuwe verordening is dat natuurlijke personen zelf controle moeten hebben over hun eigen persoonsgegevens. De AVG bevat daarom een lijst van eisen en richtlijnen die we kunnen samenvatten in drie begrippen: transparantie - betrokkenen - beveiliging. U kan uiteraard nog meerdere principes terugvinden in de ISO/IEC 29100.

Transparantie: Men vereist van de organisatie een perfect begrip en controle van de gegevensverwerking (verzameling, opslag, proces, toegangsrechten, ...). De processen moeten gedocumenteerd worden en in meeste gevallen moet de organisatie de betrokkene informeren over de verwerkingsactiviteiten (met enkele uitzonderingen).

Betrokkenen: volgens AVG (Art 4 §1), een geïdentificeerde of identificeerbare natuurlijke persoon. De verordening is gericht op de bescherming van personen en voorziet in meer rechten voor de zogenaamde betrokkene. Elke organisatie moet hier dus rekening mee houden en een proces/procedure invoeren om aan de vraag van de betrokkene te kunnen voldoen.

Beveiliging: Naast de documentatie en de rechten van de betrokkenen, moet de organisatie alle gegevens die zij verwerkt voldoende beschermen en passende beveiligingsmaatregelen treffen.

Verwerking

In de AVG (Art. 4 §2) valt nagenoeg elke actie onder de term ‘verwerking’: verzamelen, opslaan, vastleggen, versturen, raadplegen, gebruiken, bijwerken, structureren, …

De ‘verwerkingsverantwoordelijke’ (opdrachtgever tot informatieverwerking) is de partij die de informatiecategorie (of gevoeligheid, vertrouwelijkheid) van de informatie vastlegt en communiceert met de ‘ontvanger’. De verwerker is de organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

[1] Art. 3 AVG.

Om persoonsgegevens te kunnen verwerken, moeten de betrokkenen op de hoogte gebracht worden van de verwerking. Men moet hem/haar informeren over de doeleinden, hoe de gegevens worden verwerkt, welke gegevens worden verzameld, wie de gegevens zal ontvangen en welke rechten de betrokkenen hebben op het gebied van gegevensbescherming.

Wat wordt er verstaan onder 'persoonsgegevens'?

AVG Art. 4 1) definieert "persoonsgegevens" als *"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;"*

Dit houdt dus alle informatie in die direct over iemand gaat, ofwel naar deze persoon te herleiden is, zelfs indirect.

Ook digitale of technische gegevens zoals gebruikersnamen, netwerkadressen (MAC), IP-adressen, sociale media accounts en zelfs tweets die gelinkt kunnen worden aan een individuele natuurlijke persoon worden beschouwd als persoonsgegevens.

Rollen en verantwoordelijkheden

Een overheidsinstantie dient een DPO te benoemen. Zoals beschreven in AVG Art. 37 §3, kan één DPO worden aangewezen voor verschillende overheidsinstanties of overheidsorganen, met inachtneming van hun organisatiestructuur en omvang.

Daarnaast kan het werk tevens worden uitbesteed aan een externe DPO. De verantwoordelijkheid ligt ook bij het management om te voorzien in de minimale maatregelen om in overeenstemming te zijn met de AVG en hiervoor het nodige bewijs te leveren.

Zie FISP – Starterkit, voor meer informatie over de rollen en verantwoordelijkheden.

Gegevensbescherming volgens ontwerp en standaard

Volgens de AVG principes van "gegevensbescherming door ontwerp en door standaardinstellingen" wordt van een federale organisatie verwacht dat zij bij (voordat) het opstarten van een nieuw proces of project rekening houden met de laatste stand van zaken op het gebied van gegevensbescherming.[2] Door de maatregelen voor gegevensbescherming aan het begin mee te nemen in de ontwikkeling, is men eerder in regel met regelgeving omtrent gegevensbescherming en worden extra kosten vermeden als men deze maatregelen later alsnog moeten worden genomen.

Federale organisaties worden dus gestimuleerd om in het vroegste stadium van het ontwerp van de verwerkingsactiviteiten de technische en organisatorische maatregelen te treffen die nodig zijn om de beginselen inzake gegevensbescherming vanaf het begin te waarborgen. Standaard moeten federale organisaties ervoor zorgen dat persoonsgegevens worden verwerkt met het hoogste niveau van bescherming.[3] Bescherming volgens standaard kan gezien worden als een onderdeel van bescherming volgens ontwerp.

Gegevensbescherming door ontwerp

Bescherming door ontwerp stelt dat elke actie die een bedrijf onderneemt met betrekking tot de verwerking van persoonsgegevens moet worden gedaan met het oog op de bescherming van gegevens. Dit omvat interne projecten, productontwikkeling, softwareontwikkeling, IT-systemen en nog veel meer. In de praktijk betekent dit dat alle afdelingen (en niet alleen IT-afdeling) die persoonsgegevens verwerken ervoor moeten zorgen dat gegevensbescherming wordt ingebouwd in een systeem gedurende de gehele levenscyclus van het systeem of proces. Van bij de ontwikkeling van toepassingen, diensten en producten die gegevens verwerken, treft de verwerkingsverantwoordelijke dus passende technische en organisatorische maatregelen om de gegevensbeschermingsbeginselen uit te voeren.

Het startpunt van bescherming door ontwerp is een beveiligings- en privacy--beoordeling (PIA). Afhankelijk van de situatie kan het dan nog noodzakelijk zijn om een gegevensbeschermingseffectbeoordeling (GBEB, beter gekend als DPIA uit het Engels) te ondernemen. Deze kan helpen met het inzichtelijk maken van welke maatregelen vereist zijn bij het ontwerpen van een nieuwe dienst of gegevensverwerking.

Art. 35 AVG en de beslissing van het Algemeen secretariaat n°1/2019 van 16 januari 2019 verduidelijkt in welke gevallen een DPIA vereist is. [4]

De technische en organisatorische maatregelen die verder in dit document besproken worden hebben specifiek betrekking op de **bescherming van persoonlijke gegevens** en niet op het organiseren van de AVG binnen de organisatie. Maar er bestaan echter ook nog maatregelen voor bescherming door ontwerp die niet alleen op persoonlijke gegevens van toepassing (dit is **gegevensbescherming**) zijn maar op **alle soorten bedrijfsgegevens** (dus **informatiebeveiliging**). Deze blijven ook nog steeds van toepassing. Een voorbeeld hiervan is toegangscontrole waarbij men vanaf het begin de toegankelijkheid van gebruikersprofielen beperkt zodat die niet standaard toegankelijk zijn voor een onbeperkt aantal personen. Dit kan men bijvoorbeeld bereiken door:

[2] Art. 25 AVG

[3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_nl

[4] https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/01_2019_AS.pdf

- Digitale gegevenskluis,
- Fysieke toegangscontrole,
- Logische toegangscontrole,
- Authenticatie en autorisatie,
- [5]…

Op organisatorisch vlak zou men moeten overgaan op het bijhouden van een autorisatiematrix en logboeken.[6] Men moet de toegang ook opstellen op basis van een *need-to-know* en *need-to-access* principe. Wanneer het echter onmogelijk is om van bij het begin de nodige toegangscontrole in te bouwen, is er nog het alternatief van toegangslogs die achteraf gecontroleerd kunnen worden.

Gegevensbescherming door standaard:

Om de naleving van de AVG aan te kunnen tonen, moeten de federale organisaties ook **interne beleidsmaatregelen** nemen en maatregelen toepassen die voldoen aan de beginselen van gegevensbescherming door standaardinstellingen. Het basisprincipe is dat persoonsgegevens niet mogen verwerkt worden en dat verwerking in beginsel enkel kan plaatsvinden die noodzakelijk zijn voor elk specifiek doel van de verwerking. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel enkel met menselijke tussenkomst voor een beperkt aantal natuurlijke personen toegankelijk worden gemaakt. Dit kan men bijvoorbeeld bereiken door:

- Gegevens-vriendelijke standaardinstelling;
- **Informatieplicht** op elke toepassing/proces over hoe de gegevens worden verwerkt, welke de beveiligingsmaatregelen zijn, wat de finaliteit is, etc. om transparantie te garanderen;
- Er moet voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn. Dit principe van het afschermen van persoonsgegevens geldt voor alle ICT-toepassingen: van browser-instellingen tot een bedrijfs-app.
- Transparante userinterface,
- …

Op organisatorisch vlak zou men moeten overgaan tot het registreren van de toestemming (bij opt-in) en de permissies.

Verplichte beschermingsvereisten van persoonsgegevens:

Documenteren van verwerkingsactiviteiten[7]

De federale organisatie moet volgens het principe van de verantwoordingsplicht documentatie bijhouden die aantoont dat zij de bescherming van de persoonsgegevens overeenkomstig de AVG waarborgt. Alle acties en documenten die in elk stadium van de ontwikkeling van de verwerking worden uitgevoerd, moeten regelmatig worden bijgewerkt om een permanente en adequate bescherming van de gegevens te waarborgen.

[5] Voor praktische maatregelen zie het document: FISP – IAM & PAM.
[6] Voor meer informatie over logging zie FISP – Logging.
[7] Art.30 AVG.

Overzicht verwerkingsactiviteiten

Elke organisatie moet van bij de start van het project een overzicht bijhouden van de verwerkingsactiviteiten die worden uitgevoerd.[8] Zoals o.a. een beschrijving van de technische en organisatorische beveiligingsmaatregelen. Dit kan men bijvoorbeeld bereiken door:

- Register opstellen in schriftelijke vorm of elektronische vorm,
- Register van inbreuken (persoonlijke gegevenslekken)
- Register met het verwijderingsproces van persoonsgegevens
- …

Dataminimalisatie[9]:

Volgens het principe van de proportionaliteit moeten de federale organisaties vaststellen welke persoonsgegevens minimaal nodig zijn voor de opdracht/verwerking en alleen die gegevens mogen verwerkt worden. Als persoonsgegevens niet nodig zijn voor de verwerking, mogen ze niet verzameld of verwerkt worden. Dit kan men bijvoorbeeld bereiken door:

- Strikt noodzakelijke gegevens te verzamelen of overbodige gegevens direct te verwijderen;
- De toepassing van een disclaimer op elke toepassing/proces over hoe de gegevens worden verwerkt, welke de beveiligingsmaatregelen zijn, wat de finaliteit is, etc.
- De (web)invulformulieren aan te passen zodat duidelijk is wat verplicht ingevuld dient te worden en wat niet,
- …[10]

Op organisatorisch vlak zou men een duidelijke doelomschrijving met een opsomming van de noodzakelijke gegevens moeten maken.

Verwijderen/ bewaartermijnen[11]:

Voor het bewaren van persoonsgegevens zijn er grofweg 4 fases die doorlopen worden volgens de AVG (sommige modellen voorzien meer gedetailleerde stappen, maar dat gaat te ver voor het bestek van dit document.

1. **De creatiefase**: die is de start van de cyclus waar de gegevens worden aangemaakt, opgevraagd of verzameld, bij de gebruiker zelf, van de organisatie zelf of van andere organisaties (3e partijen of andere verwerkingsverantwoordelijken)
2. **De opslagfase**: de gegevens worden op een of andere manier bewaard voor later (of onmiddellijk) gebruik
3. **De gebruiksfase**:
    a. **Actief Gebruik**: dit is de periode waarin de federale organisatie de gegevens nog nodig heeft. De persoonsgegevens worden enkel verwerkt voor het bereiken van het, door de verwerkingsverantwoordelijke, bepaalde verwerkingsdoel(en). In deze fase hoeft de federale organisatie de persoonsgegevens nog niet te archiveren.
    b. **Archivering**: dit is de periode waarin de federale organisatie de persoonsgegevens misschien nog nodig heeft of wanneer beslist wordt de persoonsgegevens te archiveren. In deze fase worden de gegevens bewaard omwille administratieve redenen of wettelijke voorschriften. Bijvoorbeeld wanneer verdere verwerking noodzakelijk is met het oog op

[8] Er zijn uitzonderingen van toepassing in art.30 AVG.
[9] Art. 5, lid 1 punt C AVG.
[10] Meerdere verplichtingen kunnen ook teruggevonden worden in de “only once”- wet
[11] Art 5 lid 1 punt e AVG

archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of omwille van statistische doeleinden. Men dient dan ook rekening te houden met de archiefwet.

4. **De verwijderfase**: dit is de fase waarin de federale organisatie de persoonsgegevens op geen enkele manier (meer) nodig heeft, het verwerkingsdoel is niet meer aanwezig. In deze fase moet men ervoor zorgen dat de persoonsgegevens niet langer bewaard worden, tenminste: niet in de vorm van persoonsgegevens.

De gegevens moeten uiteindelijk gewist, vernietigd of geanonimiseerd worden met respect voor de vastgelegde wettelijke bewaartermijnen in wet- en regelgeving. De federale organisatie zal ook bewijs moeten voorzien van dit proces.

Technisch kan men aan deze beschermingsvereisten voldoen door:

- Automatisch vernietigen;
- Markeren van data na het verstrijken van de bewaartermijn;
- Sticky policies;
- Data fading;
- Bewijs van verwijdering door een log of een audit report;
- …

Op organisatorisch vlak kan men best een beleid opmaken met een overzicht van de bewaartermijnen en de omgang met e-waste (zowel oude documenten en apparaten die informatie kunnen bevatten).

Extra technische maatregelen voor de bescherming van persoonsgegevens:

Na een beveiligingsbeoordeling, PIA en eventuele DPIA kan de federale organisatie bijkomende beschermingsmaatregelen nemen. Op zijn minst één van de hieronder vermelde bijkomende beschermingsmaatregelen moet toegepast worden.

Na het implementeren van de technische en organisatorische beveiligingsmaatregelen moet de doeltreffendheid van deze maatregelen ook op gezette tijdstippen getest, beoordeeld en geëvalueerd worden.

Bovendien zal de federale organisatie de nodige maatregelen moeten nemen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te kunnen garanderen. Alsook een procedure om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.

Anonimiseren van persoonlijke gegevens:

Men kan gebruik maken van de techniek van anonimiseren om te garanderen dat het onmogelijk is om terug te keren naar de basis van de oorspronkelijke informatie.

BELANGRIJK: Anonimisatie garandeert in ALLE omstandigheden dat de identificatie van personen onmogelijk is. Wanneer door gebruik van andere bronnen identificatie mogelijk is (zelfs op een later tijdstip, met andere of nieuwere technieken), praten we over pseudonimisatie.

Dus, men moet goed opletten dat we niet meer spreken over geanonimiseerde gegevens wanneer een persoon geïdentificeerd kan worden aan de hand van een combinatie van verschillende gegevens bronnen, door middel van correlatie van de informatie,… In praktijk is echte anonimisatie erg moeilijk, en past men pseudonimisatie toe tot een niveau dat identificatie heel erg moeilijk of heel kostelijk wordt. Maar de vooruitgang van de techniek

maakt heel wat zaken mogelijk die vroeger niet bestonden. Dus dit moet goed opgevolgd worden, zodat de gegevens steeds voldoende beschermd blijven.

Versleuteling/coderen:

Encryptie kan een van de technische maatregelen zijn die worden toegepast om informatie te beschermen van bij het begin. Bij de toepassing van encryptie moet de organisatie ook rekening houden met het feit dat zij moet kunnen antwoorden op verzoeken van de betrokkene en dus snel informatie moet kunnen vinden. Dit kan men bijvoorbeeld bereiken door:

- Public key encryptie;
- Disk encryptie;
- polymorfe pseudo identifier;
- …

Voor meer praktische maatregelen zie het document: Handleiding voor cryptografie (FISPDOC03).

Pseudonimiseren van persoonsgegevens:

Dit is het vervangen van persoonlijk identificeerbaar materiaal met kunstmatige identificatiemiddelen. Dit kan men bijvoorbeeld bereiken door:

- ontdoen van directe identificerende kenmerken;
- hashing,
- data masking,
- data obfuscation,
- tokenization,
- …

Op organisatorisch vlak zou men een beleid moeten opstellen zodat men identificatie-gegevens en overige gegevens gescheiden kan houden.

Federale organisaties zouden moeten proberen deze maatregelen zoveel mogelijk toe te passen in het proces van het auditlogboek. Als de federale organisatie bijvoorbeeld als verwerker optreedt, kunnen ze alleen een taak-ID en een gebruiks-ID bewaren en de verantwoordelijke voor de verwerking vragen om de echte naam van de gebruiker te traceren. Voor meer informatie over logging zie FISP – Logging.

Logging van wie/wat/wanneer:

Logging is belangrijk om te weten wie bepaalde gegevens of een bepaald dossier heeft geconsulteerd en wanneer. Zie FISP-logging.

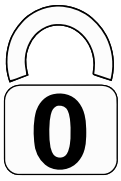
Bescherming van persoonsgegevens in de praktijk

Informatiecategorisatie

Om aan de regels te voldoen, moet elke organisatie in staat zijn te antwoorden op elk verzoek om een beroep te doen op zijn/haar rechten (toegang, wijziging, uitwissing, ...). De rubricering van de gegevens is dus een zeer nuttig en belangrijk instrument om aan dit verzoek te voldoen. Hierbij moet rekening worden gehouden met de persoonsgegevens die door de organisatie worden verwerkt. De federale organisatie moet in staat zijn om dergelijke "gevoelige" persoonsgegevens te identificeren en te lokaliseren om ze vervolgens correct te beschermen.

Om een zekere uniformiteit in de benadering van persoonsgegevens te garanderen wenst de federale overheid te werken met een aantal standaard definities van standaard datatypes. Deze persoonsgegevens met hun specifieke relatie tot de informatiecategorisatie zorgen voor een uniforme interpretatie van de noodzakelijke maatregelen die oneigenlijk gebruik, of misbruik, van persoonsgegevens moet voorkomen. Het uiteindelijke doel is op een uniforme manier persoonsgegevens zo correct en transparant mogelijk te verwerken én de rechten van ieder individu te respecteren.

Verdere informatie over de verschillende datatypes kan gevonden worden in de FISP-Starterkit.

Categorie	Generieke informatie benaming van het type persoonsinformatie
	➢ Er werden geen standaard datatypes gerelateerd aan persoonsgegevens, geïdentificeerd in de Informatiecategorie 0.
	➢ Professionele contact gegevens
	➢ Vrijetijdsbesteding en interesses ➢ Persoonlijke contact gegevens ➢ Identificatie gegevens ➢ Persoonlijke kenmerken ➢ Consumptiegewoonten ➢ Woningkenmerken ➢ Opleiding, ervaring en vorming ➢ Beroep en betrekking ➢ Financiële en fiscale gegevens ➢ Leefgewoonten ➢ Samenstelling van het gezin ➢ Locatiegegevens ➢ Contractuele detail met werkgever ➢ Evaluatie en prestaties ➢ Gegevens sociale zekerheid ➢ Rijksregisternummer, Identificatienummer van de sociale zekerheid

	➢ Fysieke, Medische of psychische gegevens en behandelingen ➢ Juridische en gerechtelijke gegevens ➢ Raciale of etnische gegevens ➢ Gegevens over seksuele geaardheid ➢ Politieke, filosofische of religieuze relaties en overtuigingen ➢ Beeld- en geluidopnamen ➢ Genetische en biometrische gegevens ➢ Statuten en vergunningen
	Specifieke informatie die onder art. 23 van de AVG valt zoals persoonlijke informatie die een invloed heeft op nationale veiligheid, openbare veiligheid, de inning van civielrechtelijk vorderingen,...

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
27/05/2019	BOSA	V0.1	Eerste draft
24/06/2019	BOSA	V0.2	Update op basis van comments
28/08/2019	BOSA	V0.3	Update op basis van comments
03/09/2019	BOSA	V0.4	Update op basis van comments van de CCB
18/09/2019	BOSA	V1.0	Update op basis van comments
7/10/2019	BOSA	V2.0	Update op basis van comments tijdens de validatie
21/11/2019	FISP Workgroup	V2.1	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP Workgroup	v2.1

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- ISO/IEC 29100,
- ISO/IEC 27001, 27002, 27701
- Gratis ISO-standaarden (waaronder ISO29100 en ISO27000)
- Verordening (EU) 2016/679 Van het Europees Parlement en de Raad/ 27 April 2016 (GDPR/AVG)
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.
- Thema dossier van de Gegevensbeschermingsautoriteit (https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming)
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_nl

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC04	*Handleiding voor logging en monitoring*
FISPDOC05	*Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)*
FISPDOC03	*Handleiding voor cryptografie*

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	*Doelstellingen en referentiemaatregelen*	*In relatie (X = Ja)*
4	*Context van de organisatie*	
5	*Leiderschap*	
6	*Planning*	
7	*Ondersteuning*	
8	*Operatie*	
9	*Evaluatie van de prestaties*	
10	*Verbeteringen*	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	*Doelstellingen en referentiemaatregelen*	*In Relatie (X = Ja)*	*Doelstellingen/ Maatregelen (Detail)*
A5	*Informatiebeveiligingsbeleid*		
A6	*Organisatie van informatiebeveiliging*		
A7	*Human Resources Veiligheid*		
A8	*Asset Management*		
A9	*Toegangscontrole*		
A10	*Geheimschrift*		
A11	*Fysieke en ecologische veiligheid*		
A12	*Operationele veiligheid*		
A13	*Beveiliging van communicatie*		
A14	*Aankoop, ontwikkeling en onderhoud van informatiesystemen*		
A15	*Relaties met leveranciers*		
A16	*Beheer van informatiebeveiligingsincidenten*		
A17	*Informatiebeveiliging in Business Continuity Management*		
A18	*Conformiteit*		