CENTRE FOR CYBER SECURITY BELGIUM

Baseline Information Security Guidelines (BSG) met AVG

Editie 2019

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

CHANCELLERY OF THE PRIME MINISTER

.be

Inleiding

Iedereen weet ongetwijfeld dat vandaag de informatie- en communicatietechnologieën (ICT) een belangrijke rol spelen in het economische en maatschappelijke leven. De goede werking van netwerken, computersystemen en software is van het allergrootste belang voor openbare instellingen en organisaties die sterk afhankelijk zijn van hun ICT-infrastructuur en bijgevolg voor het personeel dat de goede werking ervan verzekert.

Het doel van de Baseline Security Guidelines (BSG), is om minimale richtlijnen te geven onder de vorm van een gids, voor de implementatie of evaluatie van een informatiebeveiligingsplan. Ze is specifiek gericht op de Belgische overheidssector en zo hulp te bieden aan verwerkingsverantwoordelijken ondersteund door hun directie, maar ook aan beveiligingsadviseurs, gegevens-controleurs, IT-managers etc.

Het is dus niet de bedoeling om een volledige en diepgaande richtlijn uit te bouwen, want die bestaat reeds.

Deze BSG is ontwikkeld in overleg met experts van verschillende Federale Overheidsdiensten (FODs) en externe consultants, rekening houdend met bestaande normen zoals ISO/IEC 27001, ISO/IEC 27002 en ISO/IEC 27701. En uiteraard de AVG (Algemene Verordening Gegevensbescherming).

Er bestaan meerdere raamwerken ("frameworks") voor informatiebeveiliging, maar het gebruik van de ISO 2700X-norm (Information Security) als uitgangspunt heeft duidelijk een meerwaarde. Een organisatie die een ander kader gebruikt, kan eenvoudig beoordelen of de ingevoerde maatregelen verenigbaar zijn met de minimumrichtlijnen die in dit document vermeld staan.

Dit document bevat geen instructies voor praktische uitvoering, noch gedetailleerde informatie hoe dat voldaan kan worden aan de voorgestelde goede praktijken, hiervoor refereren wij naar initiatieven zoals het FISP ("Federal Information Security Policies", BOSA, 2019) of ook de Cybersecurity Reference Guide (CCB).

Het is ook belangrijk om te melden dat deze richtlijnen en raamwerken voor informatiebeveiliging niet op zichzelf staan, want ze zijn onderdeel van bedrijfsbeheer als een groter geheel.

Dat maakt dat heel wat activiteiten die hieronder worden beschreven, zoals risicobeheer, communicatie, audit & controle en continue verbetering, hergebruikt kunnen worden of geïntegreerd kunnen worden in bestaande raamwerken.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Editie 2019

In deze versie van 2019 wordt specifieke informatie voorzien om de verplichtingen te integreren die voortvloeien uit de Algemene verordening gegevensbescherming (AVG) en de wet van 30 juli 2018 betreffende de bescherming van personen met betrekking tot de verwerking van persoonsgegevens, omdat de BSG-aanpak voor de implementatie van informatiebeveiliging ook kan worden toegepast op de implementatie van de bescherming van persoonlijke gegevens.

Opgelet:

De AVG richt zich volledig op de bescherming van persoonsgegevens, die ook een juridisch aspect omvat dat niet in deze gids wordt behandeld.

Er is een verschil tussen de dekking van informatiebeveiliging op bedrijfsniveau en de gegevensbescherming in de AVG.

Informatiebeveiliging en de bescherming van persoonsgegevens zijn gebaseerd op dezelfde basis, maar de beveiliging van informatie omvat een veel breder bereik in de context van gegevensbescherming.

Een goede informatiebeveiliging binnen een bedrijfscontext omvat naast persoonsgegevens, maar ook alle andere bedrijfsinformatie.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Inhoudstafel

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

0 Document info

0.1 Versiebeheer

Versie	Beschrijving en wijzigingen
1.0	Eerste lancering van de BSG
2.0	Toevoeging van AVG inhoud

0.2 Informatiebeveiliging t.o.v. gegevensbescherming

In deze editie is er een 2e laag van informatie toegevoegd (AVG) naast de bestaande BSG, om te vermijden dat er 2 aparte documenten ontstaan.

Zoals reeds toegelicht in de inleiding, wordt er dus een verschil gemaakt tussen

- informatiebeveiliging en
- gegevensbescherming (of dataprotectie).

Om verwarring te vermijden gebruiken we "**gegevensbescherming**" **(of "dataprotectie")** om te verwijzen naar de bescherming en het beheer van **persoonsgegevens** zoals beschreven in de **AVG Art. 4.1** .

Als we de term "**informatiebeveiliging**" gebruiken, zijn dat meer algemene maatregelen die betrekking hebben op beveiliging van **bedrijfsgegevens** onder BSG of zoals vermeld in de standaard ISO/IEC 27001.

0.3 Legenda

Om een duidelijk onderscheid te maken wordt er gebruik gemaakt van kleur codes, die aangeven wanneer maatregelen relevant zijn voor een specifiek domein.

0.3.1 BSG

Inhoud die betrekking heeft op **zowel informatiebeveiliging als gegevensbescherming**, wordt in het donker, blauw, gemarkeerd.

BSG en AVG
Informatiebeveiliging & gegevensbescherming

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

0.3.2 AVG

Inhoud die **enkel** betrekking heeft op AVG wordt in het oranje gemarkeerd.

AVG specifiek
Inhoud specifiek voor gegevensbescherming (AVG)

0.3.3 Algemeen

Algemene aandachtspunten, belangrijke info, waarschuwingen, … los van de informatiebeveiliging, dataprotectie of gegevensbescherming worden in het groen gezet.

Belangrijk - Algemeen
Algemeen aandachtspunt of inhoud los van BSG of AVG

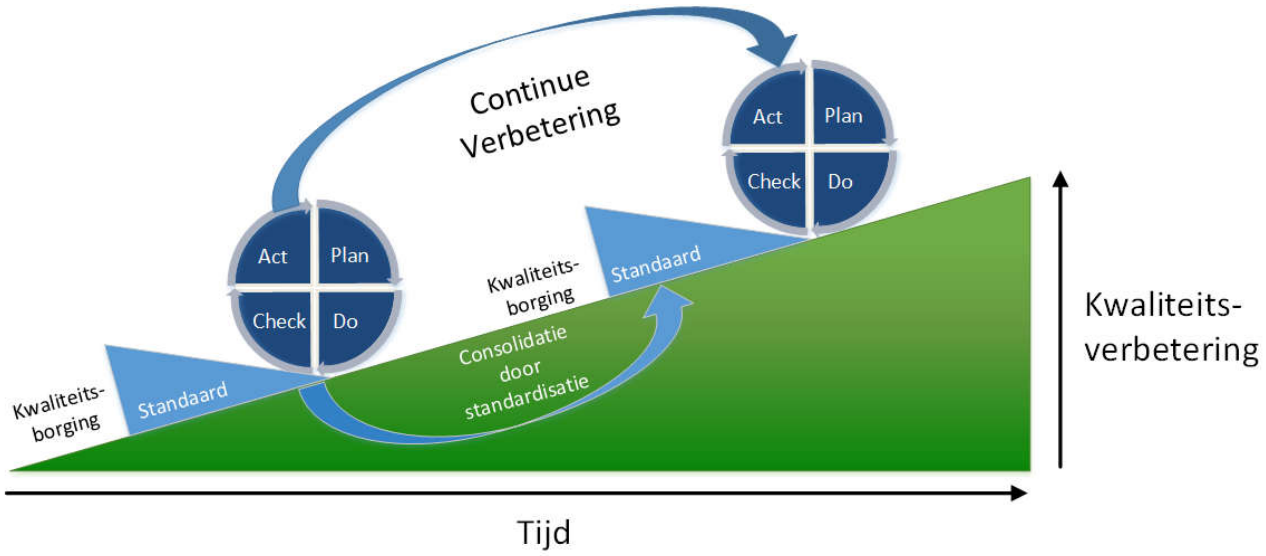
CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

1 De 4 basisprincipes van informatiebeveiligingsbeheer en data protectie

Bij de implementatie van een goed informatiebeveiligingsbeheer en ook gegevensbescherming in functie van de AVG, dienen **vier basisprincipes** in gedachten te worden gehouden:

1. Beveiligingsstrategie en ondersteuning
2. Inventaris van activa, persoonsgegevens en risicoanalyse
3. Uitvoering van veiligheidsmaatregelen
4. Evaluatie en controle van de beveiligingsmaatregelen

Deze basisprincipes zijn geïnspireerd op een gekende en veelgebruikte **kwaliteitsaanpak van informatiebeveiliging**, die bestaat uit een continue evaluatie van de uitgevoerde acties om de kwaliteit te verbeteren. Dit is gekend als het **PDCA principe** (Plan, Do, Check, Act).



Belangrijk

De continue evaluatie zorgt ervoor dat de PDCA-aanpak na de eerste implementatie een terugkerende cyclus wordt, met de bedoeling steeds te verbeteren.

AVG

De 4 principes zijn ook rechtstreeks van toepassing bij de implementatie van de AVG, zoals de Belgische Gegevensbeschermingsautoriteit (GBA) gebruikt in haar referentiemaatregelen.

Deze **vier principes** bevatten **15 aandachtspunten** die als volgt zijn geformuleerd.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

1.1 Beheersstrategie en ondersteuning

1. **De betrokkenheid van managers en de verantwoordelijken voor verwerking van gegevens** is de beste manier om het opzetten van operationele structuren, procedures en middelen te ondersteunen. Maar om de maatregelen effectief te kunnen inzetten, moeten ze worden gecommuniceerd aan alle belanghebbende partijen van de organisatie.
2. Ontwikkel een **veiligheidsbeleid, een strategie voor de informatiebeveiliging en bescherming van persoonsgegevens**, afgestemd op de strategie van de organisatie om doelstellingen te ondersteunen met inachtneming van wet- en regelgeving.
3. Stel een meerjarenplan op voor geregelde **training en sensibilisering** van alle interne én externe medewerkers en de organisatie als geheel.
4. Integreer vanaf het begin een **cultuur van veiligheid en risicoanalyse** voor alle nieuwe projecten, of het nu gaat om de ontwikkeling van nieuwe toepassingen of projecten voor bedrijfsbeheer.
5. Beschik over een **beheersplan voor grote/ernstige veiligheidsincidenten** en -crises. Onder AVG Art. 4 (12) "inbreuk in verband met persoonsgegevens" of "personal data breach" (EN)
6. Beschik over een **actief en geregeld beheer van belangrijke wijzigingen** in de omgeving.
7. Beschik over een **bedrijfscontinuïteitsplan** (BCP).

1.2 Inventaris van persoonsgegevens en risicoanalyse

8. **Identificeer de belangrijke informatiemiddelen en persoonsgegevens** (incl. hun bronnen, hun verwerking, de ontvangers, …) en de eigenaars ervan en definieer vervolgens de rollen en verantwoordelijkheden voor de hele keten van risicobeheersing.
9. **Risico's beheren** om prioriteiten vast te stellen en passende maatregelen te nemen om de risico's te verminderen (door ze op een aanvaardbaar niveau te brengen) en potentiële effecten met betrekking tot informatiemiddelen te beperken.

1.3 Uitvoering van veiligheidsmaatregelen

10. Implementeer **specifieke maatregelen** om de informatie van de organisatie te beveiligen die gevalideerd, gecommuniceerd, geïmplementeerd en herzien moet worden.
11. **Beheer de middelen** die zijn toegewezen aan informatiebeveiliging en -infrastructuur, op een effectieve en efficiënte manier, inclusief de aanwijzing van functionarissen voor informatiebeveiliging en gegevensbescherming.
12. Stel, met ondersteuning van het management, een **beleid voor de categorisering van gevoelige informatiesystemen en gegevens** vast, op basis van de principes van confidentialiteit, integriteit en beschikbaarheid (CIB, in het Engels CIA) en hun gevoeligheid op vlak van gegevensbescherming voor de gehele levensduur. Dit moet geregeld worden herzien.

1.4 Evaluatie van de beveiligingsmaatregelen

13. Voer minstens **jaarlijks** een **evaluatie van de beveiligingsmaatregelen** uit om de status van het beveiligingsplan te beoordelen, de mogelijke verbeteringen en aanvullingen ervan zijn voor elke organisatie noodzakelijk.
14. **Meet de prestaties van uitgevoerde acties** (vorige punten) maar ook de evolutie van bedreigingen en kwetsbaarheden op regelmatige tijdstippen om ervoor te zorgen dat de doelstellingen worden bereikt (cyclus van continue verbetering: PDCA).
15. Overweeg het **aanpassen van risicoanalyse en -beheer** in het licht van audits en bewezen incidenten en belangrijke wijzigingen die **impact** hebben op de activiteiten.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

2 Beheersstrategie en ondersteuning

2.1 De betrokkenheid van de topmanagers

Jouw beveiligingsplan voor inforrmatiebeveiliging en gegevensbescherming en de prioriteiten daarvan moeten door het **topmanagement van jouw organisatie** worden gepresenteerd, goedgekeurd, gevalideerd en ondersteund, als eindverantwoordelijke voor de informatiebeveiliging en data protectie.

Daartoe moet elke voorgestelde maatregel een vermelding bevatten van de prioriteit ervan en de nodige middelen.

Het is belangrijk ervoor te zorgen dat dit plan aansluit bij de **strategie en operationele doelstellingen** van jouw organisatie, anders wordt het door het management verworpen.

In jouw ontwerp van veiligheidsplan duidt je het huidige beveiligingsniveau en het gewenste niveau na uitvoering van jouw plan aan. De verantwoordelijkheid van het management (de verwerkingsverantwoordelijke) moet worden benadrukt, met name in verband met de aanvaarding van het risico door het management.

Eenmaal goedgekeurd door het management zal dit plan moeten worden geïntegreerd in de operationele prioriteiten van de organisatie en zal dit moeten worden gecommuniceerd naar de hele organisatie en de belanghebbende partijen voor samenwerking.

2.2 De veiligheidsstrategie

Het beheer van informatiebeveiliging en data protectie vereist dat het **management betrokken** is, wat niet alleen een veiligheidscultuur maar ook goede praktijken en beveiligingsmaatregelen bevordert.

Maar zelfs al is het eenvoudiger om een technische oplossing te kopen dan om te proberen de cultuur van de organisatie te veranderen, dan nog zal geen enkele technische oplossing de **efficiëntie en creativiteit van een menselijke oplossing** overtreffen.

Belangrijk

Mensen zullen maar hun steentje bijdragen aan de verbetering van de beveiliging als de bedrijfscultuur dit mogelijk maakt en stimuleert.

Dus het goed voorbeeld van het management is daarvoor essentieel.

Informatiebeveiliging en gegevensbescherming beheren maakt deel uit van een goed beheer van de organisatie. Het voorziet het management van strategische aansturing, zorgt ervoor dat doelstellingen worden bereikt, risico's adequaat worden beheerst en operationele middelen effectief worden beheerd. Het meet ook het succes en/of het falen van het beveiligingsprogramma.

Voor een effectief informatiebeheer is het voor het management van belang een kader te creëren om richting te geven aan de ontwikkeling en de uitvoering van het informatiebeveiligingsplan.

Dit stelt de organisatie in staat haar kritieke activa (infrastructuur, data etc.) te beheren en tegelijkertijd te beschermen tegen belangrijke risico's.

Om deze strategie beter af te stemmen op de doelstellingen van de organisatie, zal de operationele strategie essentiële elementen voor risicoanalyse moeten bevatten, zoals operationele procedures en kritische middelen voor de informatiebeveiligingsstrategie.

Beveiligingsmaatregelen zijn het resultaat van risicoanalyse en definiëren de grote lijnen van het beveiligingsprogramma van de organisatie: de benodigde middelen, beperkingen etc.

De ontwikkeling van het informatiebeveiligingsprogramma moet ook instrumenten voorzien voor de evaluatie van de getroffen maatregelen, het nazicht en de eventuele aanpassing ervan.

Een **volledige en regelmatige voortgangsrapportage** aan de leidinggevenden zal hen in staat stellen te beslissen over aanpassingen en corrigerende maatregelen om de veiligheidstoestand te bereiken die door de organisatie vereist is.

Het informeren van managers stelt hen in staat de middelen die nodig zijn voor informatiebeveiliging te beoordelen en daarmee de minimaal te nemen maatregelen voor informatiebeveiliging te accepteren.

Deze minimummaatregelen zijn aangepast aan het belang van activa die beschermd moeten worden en de gevoeligheid ervan. Deze basismaatregelen zijn gedefinieerd in termen van middelen, procedures en technische middelen; ze zijn vaak gebaseerd op normen en naleving van nationale en sectorale wet- en regelgeving.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

3 Essentiële activa inventariseren & risicoanalyse

3.1 Definitie essentiële activa

Voor informatiebeveiliging worden de essentiële activa in brede zin beschouwd als 'alle middelen die een waarde hebben voor de organisatie en die moeten worden beveiligd'. Daartoe is een duidelijk inzicht noodzakelijk in de waarde en het belang van de verwerkte gegevens (cf. categorisatie informatie).

Dit beperkt zich niet enkel tot IT-infrastructuur of tastbare middelen, maar ook tot gegevens, en mensen. Het kunnen bovendien ook ontastbare middelen zijn, zoals processen, procedures, bepaalde werkwijzen, kennis en expertise etc.

De toepassing van **dataprotectie** (AVG) verschilt hierin, want de definitie van de **essentiële activa is gedefinieerd** in de **AVG** zelf.

Meer specifiek Art.4.1 bepaalt de inhoud van "**persoonsgegevens**". Daarnaast bevat AVG Art.9.1 ook de definitie van **bijzondere categorieën** van persoonsgegevens.

3.2 Inventaris van activa

De eerste stap is het **inventariseren van de bedrijfsmiddelen en de persoonsgegevens die essentieel zijn** voor de bedrijfsvoering (ref. verwerkingsactiviteiten) van jouw organisatie.

We raden bijvoorbeeld aan om te beginnen met "essentiële activa" die bekend en geïdentificeerd zijn door het management.

Verschillende iteraties van het plan zullen toelaten om deze inventaris geleidelijk op te bouwen, te verrijken, aan te vullen, uit te breiden.

De AVG vereist ook een inventaris van de verwerking van persoonsgegevens "register van verwerkingsactiviteiten". De minimaal vereiste informatie is beschreven in artikel 30 van de AVG. In de meeste gevallen zal een gegevensverwerking overeenkomen met een informatiesysteem en de geïdentificeerde activa zullen overeenkomen met de elementen (IT, personeel, infrastructuur, ...) die nodig zijn om deze behandeling uit te voeren.

3.2.1 Stappen

De inventaris opmaken:

- Definieer/identificeer in samenwerking met het management en de verschillende afdelingen de "essentiële activa".
- Ontmoet de mensen die verantwoordelijk zijn voor deze verschillende activa om ze beter te identificeren en te definiëren.
- Stel er een lijst van op.
- Laat deze lijst formeel goedkeuren door het management, zodat het betrokken kan worden bij jouw proces (bijvoorbeeld via een goedkeuringsrapport of een document ondertekend door het management).

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

3.2.2 Resultaat

Hieronder volgt een niet-exhaustieve lijst van belangrijke soorten activa die in elke organisatie bestaan:

- de **primaire activa**, die essentieel zijn voor het voortbestaan van de organisatie. Dit zijn onder meer:
  - informatie, gegevens, diensten, kernprocessen, bepaalde werknemers en hun functies;
  - persoonsgegevens die absoluut nodig zijn om de kerndienst van de organisatie te verzekeren
- secundaire **activa,** ter ondersteuning van primaire activa als:
  - IT systemen, netwerk, telecommunicatie, …
  - Persoonsgegevens die nodig zijn voor ondersteunende processen zoals nieuwsbrieven, marketing,…

In plaats van een exhaustieve lijst te hebben, focus je beter op de essentie wanneer je die oefening start.

Het is beter om het proces te starten met slechts een beperkt aantal activa, dan te proberen ze allemaal op te sommen, omdat er een groot risico bestaat dat wanneer je de oefening hebt voltooid, deze al verouderd zal zijn.

Belangrijk
Het is belangrijk om het proces op gang te brengen en dan continu te verbeteren

Een benadering voor de identificatie van activa is te vinden in de Methode voor geoptimaliseerde Risicoanalyse (Monarc)[2]. Een nog meer gedetailleerde aanpak is ook te vinden in de ISO/IEC 27005-standaard.

[2] http://monarc. lu/

3.3 Risicoanalyse (in 6 punten)

Voor elk essentieel onderdeel is het belangrijk om een risicoanalyse te maken.

We willen erop wijzen dat Afdeling 3 (Art. 35-36) van de EU-AVG de behoefte aan een risicoanalyse verduidelijkt voor elke verwerking van persoonsgegevens die gevaar lopen.

Terwijl in het kader van een gebruikelijke risicobeheerbenadering de risico's voor de organisatie worden overwogen. In de context van de AVG moet rekening worden gehouden met de risico's voor de personen wier informatie wordt verwerkt. De behandeling van deze twee aspecten is complementair. Ze zullen gezamenlijk worden aangepakt en zullen meestal leiden tot een gemeenschappelijke risicobehandeling.

3.3.1 Bepaal de context van jouw organisatie

- **Risicoprofiel organisatie** (interne & externe factoren)
  - Wat is de specifieke context van jouw specifieke organisatie/sector?
  - Eigenschappen van de organisatie?
  - Interne en externe factoren die risico beïnvloeden?
  - Welke soorten gegevens worden verwerkt (persoonlijke gegevens en anderen)
  - Wat zijn voor elk type gegevens de risico's voor de organisatie en voor de betrokken personen?
- **Risico-appetijt** van organisatie (keuze van bedrijf)
  - Wat is het aanvaardbare risiconiveau voor jouw organisatie?
  - Quel est le niveau de risque acceptable pour les personnes concernées?

3.3.2 Contextmodellering

- Identificatie van essentiële activa
  - Verzamel informatie zoals bronnen, processtromen, infrastructuren, databanken, octrooien, sleutelpersonen, overdracht van gegevens aan derden, etc.
  - Verzamel contractinfo met derden: leveranciers, onderaannemers, IT-providers, cloud etc., elke externe partij die infrastructuur, applicaties of databases voor jouw organisatie beheert.
- Identificatie van risico's, kwetsbaarheden, bedreigingen etc.
  - Identificeer mogelijke risico's in termen van confidentialiteit, integriteit, beschikbaarheid (CIB of beter gekend als CIA) , traceerbaarheid, onweerlegbaarheid en authenticiteit van gegevens, evenals de compliance risico's van de GDPR (wettigheid, evenredigheid, kansen, transparantie, exact, update, ...).
  - Het begrip "risico" wordt in het algemeen omschreven als
    - de mogelijkheid ("waarschijnlijkheid")
    - dat een bepaalde "dreiging" (uitbuiten van een "kwetsbaarheid") zich zal voordoen
    - met een bijzondere impact ("ernst") tot gevolg.
  - Een risico wordt vaak uitgedrukt in termen van de combinatie van de **gevolgen** van een gebeurtenis (inclusief veranderingen in omstandigheden) en de **waarschijnlijkheid** van een gebeurtenis.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

- Een proces waarbij de resultaten van de risicoanalyse worden vergeleken met de risicocriteria om te bepalen of het risico en/of de betekenis ervan al dan niet aanvaardbaar is.

3.3.3 Risicobeoordeling en behandeling

- Identificeer de organisatorische, operationele en technische beveiligingsmaatregelen die reeds **van kracht** zijn om de activa te beveiligen.
- Het identificeren van aanvullende organisatorische, operationele en technische beveiligingsmaatregelen om de **beveiliging te verbeteren**.
- Beoordeel de omvang van het restrisico. Is het op een aanvaardbaar niveau voor jouw organisatie?

Bij risicomanagement kan een onderscheid worden gemaakt tussen een "inherent" en een "residueel" risico.

- **Inherent risico** verwijst naar de waarschijnlijkheid dat een negatieve impact optreedt wanneer er geen beschermende maatregelen worden genomen.
- **Residueel of restrisico** verwijst naar de waarschijnlijkheid dat er een negatieve impact kan optreden, ondanks de maatregelen die genomen zijn om het (inherente) risico te beïnvloeden (beperken).

De analyse van het gewenste residueel risico helpt bij het selecteren en ontwikkelen van acties/maatregelen die het residueel risico kunnen reduceren tot het gewenste niveau, zoals gedefinieerd door de asset en risico-verantwoordelijken..

3.3.4 Uitvoering van maatregelen

De uitvoering van de maatregelen kunnen op drie niveaus worden uitgevoerd volgens het PPT-principe:

1. **P**ersonen ("People");
2. **P**rocessen en procedures ("Processes");
3. **T**echnologie of technische infrastructuur ("Technology or Systems").

3.3.5 Monitoring: evaluatie van de uitvoering van maatregelen en het effect ervan op risicobeperking

Het is niet voldoende om eenmalig maatregelen in te voeren, ze moeten op geregelde tijdstippen opgevolgd worden en waar nodig bijgestuurd worden.

3.3.6 Verbeteren van de risicoanalyse met nieuwe activa (maatregel 1)

Jouw risicoanalyse is een dynamisch element dat voortdurend geactualiseerd moet worden in het licht van incidenten, verwerkingsmodificaties, gereedschapsonderhoud, aanpassing van essentiële bedrijfsmiddelen, wettelijke of regelgevende aanpassingen etc.

3.4 Welke methode te gebruiken?

Een risicoanalyse is terug te vinden in de methode voor geoptimaliseerde risicoanalyse ("Monarc"). Een meer algemene aanpak is ook te vinden in ISO 27005.

Jouw risicoanalyse kan heel eenvoudig zijn, maar ze kan ook gedetailleerd zijn.

Het hangt af van de grootte van jouw organisatie, de complexiteit van de projecten en de gevoeligheid van de gegevens die je verwerkt, de beschikbaarheid van expertise, de beschikbare tijd en het budget.

Onderschat het werk niet, omdat de risico's aanzienlijk kunnen zijn zelfs als een project eenvoudig lijkt. Er is dus geen evenredigheid tussen de omvang van het project en de risico's die aan dit project verbonden zijn. Om de nauwkeurigheid en volledigheid van jouw risicoanalyse te controleren, moet je deze door verschillende mensen in jouw organisatie laten nakijken.

Als algemene regel geldt dat elke organisatie vrij is om de methodologie te kiezen die ze wenst te gebruiken.

Maar het gebruik van een vergelijkbare methode door andere partijen kan interessant zijn. Op die manier kunnen resultaten vrij eenvoudig vergeleken worden, wat erg waardevol is voor een goede implementatie.

Het resultaat van jouw risicoanalyse vormt de basis van jouw beveiligingsplan. Hiervoor moet je de beveiligingsmaatregelen vaststellen die moeten worden genomen om een implementatieplan op te stellen dat gevalideerd moet worden door het management.

Deze benadering is ook van toepassing op gegevensbescherming. Zoals hierboven vermeld, is het echter belangrijk op te merken dat risicoanalyse in het kader van de AVG speciale aandacht krijgt in de vorm van een Data Protection Impact Assessment (DIA).

Voor de implementatie van de AIPD wordt vaak verwezen naar ISO29134 (Privacy Impact Assessment). Het goede nieuws is dat het perfect past in de bredere geschiedenis van IT-risicobeheer (ISO27005) en dat Monarc perfect is uitgerust om het in praktijk te brengen. De recente publicatie van ISO / IEC 27701: 2019 (uitbreiding van ISO / IEC 27001 en ISO / IEC 27002 tot privacybeheer - vereisten en richtlijnen) maakt de integratie van ISO / IEC 27701 mogelijk: informatie met gegevensbescherming.

In hun aanbeveling over de DPIA verwijst de DPA ook naar deze standaard, hoewel ze benadrukken dat elke verwerkingsverantwoordelijke vrij blijft in zijn keuze. Meer informatie hierover:

https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf (Randnummer 54 en bijhorende voetnoot 91.)

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

3.5 Integratie van Risicoanalyse in het projectmanagement

In elk ontwikkelingsproces van jouw project moet in elke fase van het project aandacht worden besteed aan veiligheid. Zorg ervoor dat je projectmanagementbeleid aangepast is aan het Project Managementniveau om de risicoanalyse en beveiligingsmaatregelen op te nemen die moeten worden geïmplementeerd.

Vergeet ook niet dat de risicoanalyse van ICT-systemen al vanaf het begin van het project is uitgevoerd om een nieuwe oplossing te ontwikkelen ("**security-by-design** & **dataprotection-by-design**") en dus een evolutionair karakter heeft! Dat betekent dat ze vaak onderhevig is aan wijzigingen in de loop van het project.

In de context van de AVG komt deze zorg om risico's te beheersen tot uiting in de eis van bescherming van persoonsgegevens vanaf de ontwerpfase en standaard (artikel 25 AVG)

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

4 Uitvoering van veiligheidsmaatregelen

Minimale beveiligingsmaatregelen worden aanbevolen voor elke organisatie, ongeacht de grootte. Sommige zullen niet van toepassing zijn in het kader van de organisatie, maar omdat deze normen voor de hele openbare dienst worden opgesteld, zijn ze aanpasbaar aan de grootte en context van jouw organisatie.

Om een link te houden met de hieronder beschreven metingen volgen we de volgorde van de ISO 27001-norm waaraan ze zijn ontleend.

4.1 Veiligheidsbeleid

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie moet een informatie-beveiligingsbeleid hebben dat is goedgekeurd en ondersteund wordt door het management.	Elke organisatie voert een bijgewerkt informatiebeveiligings- en dataprotectie-beleid (of meerdere) uit, dat door het top management is goedgekeurd, ondertekend en ondersteund.
	Het informatiebeveiligingsbeleid is afgestemd op het dataprotectie-beleid en omgekeerd.
	Het beleid voor informatiebeveiling en dataprotectie voor betrokken partijen beschikbaar en consulteerbaar zijn.
	Het top management moet regelmatig op de hoogte worden gehouden van de stand van zaken met betrekking tot de uitgevoerde maatregelen.
	Het beleid voor informatiebeveiliging en dataprotectie moet minstens 1 maal per jaar door het management geherevalueerd worden zodat het relevant blijft, in lijn met de realiteit.

4.2 Organisatie van beveiliging en data protectie

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie zal een **risicomanagement-systeem** opzetten.	Een risicobeheerproces wordt gedocumenteerd, goedgekeurd en periodiek geëvalueerd.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	Er zal een register worden bijgehouden van de activa en toepasselijke risico's. De genomen maatregelen (vermindering, behoud, overdracht, vermijding) zullen worden bijgehouden.
Informatiebeveiliging zal worden geïntegreerd in het **projectmanagement (veiligheid per ontwerp – "Security by design")** om veiligheids-aspecten zo snel mogelijk te integreren.	Een gedocumenteerd risicobeheersingsproces voor informatiebeveiliging zal worden geactualiseerd en geïmplementeerd.
Om kennis te actualiseren en de uitwisseling van informatiebeveiligingstrends te bevorderen, zal het noodzakelijk zijn deel te nemen aan gespecialiseerde fora en gebruikersgroepen die zich bezighouden met informatiebeveiliging.	Er zal technisch toezicht worden uitgeoefend op fora en gebruikersgroepen die gespecialiseerd zijn in informatiebeveiliging.
Om ervoor te zorgen dat deze organisatorische maatregelen worden uitgevoerd, informeert elke organisatie haar personeel en derden die onder haar verantwoordelijkheid werken.	Er wordt een veiligheidsrisico-opleidingsplan ontwikkeld, bijgewerkt en opgevolgd.
	Het informatiebeveiligingsplan is beschikbaar en consulteerbaar voor de betrokken mensen.
	Voortdurende training van personeel en derden met betrekking tot het beveiligings- en gegevensbeschermingsbeleid, alsmede een sanctieprocedure voor niet-naleving zal worden geïmplementeerd.
Elke organisatie zorgt ervoor dat een informatiebeveiliger met een duidelijk mandaat wordt aangewezen en gemandateerd.	Er zal een verantwoordelijke voor informatiebeveiliging met een duidelijk mandaat wordt aangewezen en gemandateerd.
Elke organisatie beschikt over een **dashboard** om het **beveiligingsniveau te meten en op te volgen** aan de hand van de doelstellingen van de strategie van de organisatie.	Een dashboard wordt beoordeeld, gepresenteerd aan het management en gebruikt om de veiligheidstoestand van de organisatie te beoordelen.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Er zullen een **gedragscode en goede praktijken** voor het gebruik van informatiesystemen worden ontwikkeld, goedgekeurd en gecommuniceerd.	Stel een gedragscode op voor elke gebruiker bij het selecteren, beheren en ontsluiten van jouw medewerkers en zeker voor degenen die toegang hebben tot gevoelige gegevens of kritieke systemen.
	Deze gedragscode dient de volgende elementen te bevatten: ▪ Toegangscontrole/autorisatiebeheer ▪ Intrekking van rechten ▪ Confidentialiteit van gegevens. ▪ Fysieke toegang tot gebouwen en infrastructuur? ▪ Toegangssystemen en confidentialiteit van toegangsgegevens ▪ Procedures om het juiste gebruik te bepalen van werkinstrumenten die ter beschikking gesteld worden (zoals mobiele apparaten, telewerk, gegevensclassificatie etc.) ▪ Welke maatregelen zijn genomen om de activiteiten te controleren (toegang, vernietiging van opslag, toegang op afstand, loggen)?
	De gedragscode **publiceren, communiceren en de gedragscode regelmatig herhalen** (door middel van bewustmakingscampagnes).
Er zal een informatie- en opleidingsplan worden goedgekeurd.	Het plan moet betrekkingen met derden en autoriteiten omvatten.
	Er zal een veiligheidscultuur worden gedefinieerd en bevorderd, met de integratie van veiligheid in ontwikkelingsprocessen.
Elke organisatie moet de taken en verantwoordelijkheden van de verschillende actoren in de informatiebeveiliging identificeren.	Een identificatie van de rollen en verantwoordelijkheden met betrekking tot de bescherming van gegevens, en ook de structuur van de organisatie zijn essentiële instrumenten om de vereiste taken en activiteiten voor de uitvoering van dit plan te kunnen evalueren (definitie van een RACI-matrix bv.).

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie zal een risico-managementsysteem opzetten voor het beheer van persoonsgegevens.	Een risicobeheerproces voor beheer van persoonsgegevens wordt gedocumenteerd, goedgekeurd en periodiek geëvalueerd. Dit kan zo nodig verenigd worden met het risicobeheerssysteem voor informatie-beveiliging.
	Er wordt een classificatie opgezet die persoonsgegevens opdeelt in verschillende categorieën, die elk gepast beschermd moeten worden ▪ *bijzondere categorieën van persoonsgegevens* (zoals gedefinieerd in AVG Art. 9) ▪ Gevoelige persoonsgegevens (oa financiële gegevens, …) ▪ Normale persoonsgegevens ▪ Geen persoonsgegevens
Opzetten en beheren van het AVG verwerkingsregister	(Ref AVG Art 30.) Er zal een register in de zin van artikel 30 AVG worden bijgehouden van de verschillende verwerkingsprocessen, incl.: ▪ De contactgegevens van de verwerkings-verantwoordelijke en medeverant-woordelijke ▪ Contact gegevens van DPO ▪ Verwerkingsdoeleinden ▪ Categorie van verwerkte data ▪ Categorie van betrokkenen ▪ Toepasselijke beschermingsmaatregelen ▪ …

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	Er wordt een **levenscyclus van de persoonsgegevens gedefinieerd**, inclusief ▪ Creatie ▪ Verzamelen van gegeven ▪ Verwerking ▪ Transport en distributie ▪ Opslag ▪ Archivering ▪ Vernietiging ▪ …
	Het AVG verwerkingsregister bevat ook ▪ Bron van gegevens ▪ Methode verwerving van data ▪ Verwerkingsgrond ▪ Type verwerking ▪ (categorie van) ontvangers van gegevens ▪ … Meer gedetailleerde informatie is vinden in de aanbeveling van de GBA, die op het einde van dit hoofdstuk wordt toegelicht.
Elke organisatie zorgt ervoor dat een functionaris voor gegevensbescherming (verder DPO genoemd) met een duidelijk mandaat wordt aangewezen en gemandateerd.	AVG Art. 37 *"De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;"*
	Er zal een functionaris voor gegevens-bescherming met een duidelijk mandaat worden benoemd.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Dataprotectie zal worden geïntegreerd in het projectmanagement (gegevensbescherming per ontwerp) om veiligheidsaspecten zo snel mogelijk te integreren.	GDPR Art. 25 vereist het principe van *"Gegevensbescherming door ontwerp en door standaardinstellingen "* Daarom is het belangrijk om bij de opstart van nieuwe projecten of de aanpassing van bestaande operaties, gegevensbescherming mee op te nemen.
Om kennis te actualiseren en de uitwisseling van dataprotectie-trends te bevorderen, zal het noodzakelijk zijn deel te nemen aan gespecialiseerde fora en informatiekanalen die zich bezighouden met gegevens-bescherming.	De nodige taken en agenda's worden toegewezen, gepland en uitgevoerd om deel te nemen aan fora, activiteiten die gespecialiseerd zijn in dataprotectie.
	De nodige taken en agenda's worden toegewezen, gepland en uitgevoerd om informatie te consulteren op nieuwsbrieven, blogs, online fora, enz… die up-to-date informatie leveren over dataprotectie.
Om ervoor te zorgen dat de nodige organisatorische maatregelen worden uitgevoerd, informeert elke organisatie haar personeel en derden die onder haar verantwoordelijkheid werken.	Er wordt een dataprotectie-opleidingsplan ontwikkeld, bijgewerkt en opgevolgd.
	Voortdurende training van personeel en derden met betrekking tot het beveiligings- en gegevensbeschermings-beleid, alsmede een sanctieprocedure voor niet-naleving zal worden geïmplementeerd.
Elke organisatie beschikt over een dashboard om het dataprotectie-niveau te meten en op te volgen aan de hand van de doelstellingen van de strategie van de organisatie.	Een dashboard wordt beoordeeld, gepresenteerd aan het management en gebruikt om de toestand van de dataprotectie in de organisatie te beoordelen. (incl. aantal wijzigingen, interne & externe incidenten, data lekken, aantal aanvragen voor (onrechtmatige) consultatie…)

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Er zullen een richtlijn en goede praktijken voor het gebruik van persoonsgegevens worden ontwikkeld, goedgekeurd en gecommuniceerd.	Stel richtlijnen op voor elke gebruiker bij het selecteren, beheren en ontsluiten van jouw medewerkers en zeker voor degenen die toegang hebben tot gevoelige gegevens of kritieke systemen.
	▪ Deze richtlijnen dienen de volgende elementen te bevatten: ▪ Toegangscontrole/autorisatiebeheer ▪ Intrekking van rechten ▪ Confidentialiteit van gegevens. ▪ Fysieke toegang tot gebouwen en infrastructuur? ▪ Toegangssystemen en confidentialiteit van toegangsgegevens ▪ Procedures om het juiste gebruik te bepalen van werkinstrumenten die ter beschikking gesteld worden (zoals mobiele apparaten, telewerk, gegevensclassificatie etc.) ▪ Welke maatregelen zijn genomen om de activiteiten te controleren (toegang, vernietiging van opslag, toegang op afstand, loggen)?
	Het is belangrijk om de richtlijnen te communiceren en regelmatig te herhalen (door middel van bewustmakingscampagnes).
Er zal een informatie- en opleidingsplan worden goedgekeurd.	Het plan moet betrekkingen met derden en autoriteiten omvatten.
	Er zal een veiligheidscultuur worden gedefinieerd en bevorderd, met de integratie van veiligheid in ontwikkelingsprocessen.
Regels voor de toegang tot gegevens via remote toegang (telewerk) worden bepaald.	Een toegangsprocedure voor gegevens-verwerking wordt opgesteld.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie moet de taken en verantwoordelijkheden van de verschillende actoren in de gegevensbescherming identificeren.	Een identificatie van de rollen en verantwoordelijkheden met betrekking tot de bescherming van gegevens, en ook de structuur van de organisatie zijn essentiële instrumenten om de vereiste taken en activiteiten voor de uitvoering van dit plan te kunnen evalueren (definitie van een RACI-matrix bv.).

4.2.1 AVG Verwerkingsregister

Zie aanbeveling GBA (vanaf randnummer 38) :

- https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_06_2017_0.pdf

Het is belangrijk om onderscheid maken tussen de informatiegegevens die krachtens de AVG zelf in het register moeten staan (opgesomd in artikel 30.1 AVG) en informatie waarvan de vermelding nuttig en aan te raden is, maar niet verplicht.

Zie ook bladzijde 15 van de KMO-brochure van GBA:

- https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/KMO_NL_update.pdf

4.3 Veiligheid van personeel

Veiligheidsmaatregel	Minimaal toe te passen maatregels
Er zal een beleid voor het management van medewerkers (intern en/of extern) worden gedefinieerd.	Er zullen procedures worden ontwikkeld voor de volgende aspecten: Vóór aanwerving: ▪ Aanwervingsprocedures en bijbehorende maatregelen. Tijdens het werk: ▪ Alle interne en externe medewerkers dienen zich te houden aan de gedragscode van de organisatie. Beëindiging of verandering van dienstverband: ▪ Verantwoordelijkheden en verplichtingen voor informatiebeveiliging blijven bestaan na beëindiging of verandering van dienstverband en deze voorwaarden moeten duidelijk worden gecommuniceerd en geïntegreerd in het werknemersmanagementproces (intern of extern).
Arbeidsreglement	Er moet een beleid gedefineerd worden die duidelijk de veranwoordelijkheiden van de organisatie, de interne en externe medewerkers vastlegt wat betreft informatiebeveiling en dataprotectie.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Het beleid voor werknemers(intern en extern) bevat een goede legale en/of contractuele bescherming van de persoonsgegevens	De organisatie houdt rekening met en implementeert de regels ter bescherming van de rechten en vrijheden van haar werknemers en ambtenaren zoals vastgesteld in de toepasselijke nationale regelgeving in uitvoering van artikel 88 AVG.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Aanwervingsprocedure	In de hele cyclus van de medewerkers, van aanwerving tot ontslag moet er voldoende aandacht gespendeerd worden aan de bescherming van de persoonsgegevens
Arbeidsreglement	Zie ISO27701 (vertaald) ***"6.10.2.4 Confidentiality or non-disclosure agreements*** *De controle, implementatiebegeleiding en andere informatie vermeld in ISO / IEC 27002: 2013, 13.2.4 en de volgende aanvullende richtlijnen zijn van toepassing:* ***Aanvullende implementatierichtlijnen voor 13.2.4, vertrouwelijkheids- of geheimhoudings-overeenkomsten van ISO / IEC 27002: 2013 is:*** *De organisatie moet ervoor zorgen dat personen die onder haar controle opereren met toegang tot PII een geheimhoudingsplicht hebben. In de vertrouwelijkheidsovereenkomst, ongeacht of deze deel uitmaakt van een contract of afzonderlijk, moet worden gespecificeerd hoe lang aan de verplichtingen moet worden voldaan.* *Wanneer de organisatie een PII-processor is, moet een vertrouwelijkheidsovereenkomst, in welke vorm dan ook, tussen de organisatie, haar werknemers en haar agenten ervoor zorgen dat werknemers en agenten zich houden aan het beleid en de procedures met betrekking tot gegevensverwerking en -bescherming."*

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

4.4 Bewustmaking, opleiding, training & communicatie

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Er zal een **opleidings- en trainingsplan** worden gedefinieerd, zodat alle medewerkers van de hele organisatie, zowel intern als extern, de nodige informatiebeveiligingsopleiding krijgen, voor zover relevant voor hun functie, en op geregelde tijdstippen op de hoogte worden gehouden van aanpassingen van de richtlijnen en procedures.	Er zullen procedures worden ontwikkeld voor de volgende aspecten: ▪ Een programma om bewustmaking over informatiebeveiliging bij de medewerkers, intern en extern, mogelijk te maken. ▪ Het programma moet op geregelde tijdstippen worden herhaald (liefst 1 of 2x per jaar of meer), zodat ook nieuwe medewerkers tijdig opgenomen worden in het programma. ▪ Deze informatie moet steeds op een eenvoudige, vlotte manier toegankelijk zijn voor de medewerkers.
Er zal een communicatieplan worden gedefinieerd, zodat alle belanghebbende partijen van de organisatie, zowel intern als extern, de nodige informatiebeveiligingsinformatie ontvangen, voor zover van toepassing, en op geregelde tijdstippen op de hoogte worden gehouden van aanpassingen van de richtlijnen en procedures.	Er zullen procedures worden ontwikkeld voor de volgende aspecten: ▪ Identificatie van de betrokken partijen en de gepaste manier van communicatie. ▪ Plan om partijen op geregelde tijdstippen op de hoogte te houden van aanpassingen van de richtlijnen en procedures.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Vademecum met GDPR terminologie	Als onderdeel van het veiligheidsbeleid is er een vademecum beschikbaar voor de betrokken partijen dat de gebruikte terminologie i.v.m. de implementatie van de AVG toelicht en consolideert, zodat iedereen dezelfde woordenschat gebruikt.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Er zal een opleidings- en trainingsplan worden gedefinieerd, zodat alle medewerkers van de hele organisatie, zowel intern als extern, op geregelde tijdstippen de nodige opleiding en training krijgen ▪ **over AVG en dataprotectie,** ▪ **voor zover relevant voor hun functie,** ▪ **hun rol en verantwoordelijkheid daarin,** **en op de hoogte worden gehouden van aanpassingen van de richtlijnen en procedures.**	Er zullen procedures worden ontwikkeld voor de volgende aspecten: ▪ Een programma om bewustmaking over AVG en gegevensbescherming bij de medewerkers, zowel intern als extern, mogelijk te maken. ▪ Het programma moet op geregelde tijdstippen worden herhaald (liefst 1 of 2x per jaar of meer), zodat ook nieuwe medewerkers tijdig opgenomen worden in het programma. ▪ Deze informatie moet voor elk van de medewerkers ○ duidelijk verstaanbaar zijn ○ aangepast zijn aan het niveau van de medewerker ○ steeds op een eenvoudige, vlotte manier toegankelijk zijn. ▪ Het rapporteren van mogelijke beveiligingsincidenten moet mogelijk gemaakt worden, zonder dat medewerkers hiervoor afgestraft worden of zich blootstellen aan wraakacties van medewerkers of hiërarchische oversten.
Er zal een communicatieplan worden gedefinieerd, zodat alle belanghebbende partijen van de organisatie, zowel intern als extern, de nodige dataprotectie-informatie ontvangen, voor zover van toepassing, en op geregelde tijdstippen op de hoogte worden gehouden van aanpassingen van de richtlijnen en procedures.	Er zullen procedures worden ontwikkeld voor de volgende aspecten: ▪ Identificatie van de betrokken partijen en de gepaste manier van communicatie. ▪ Plan om partijen op geregelde tijdstippen op de hoogte te houden van aanpassingen van de richtlijnen en procedures. ▪ Plan op partijen op geregelde tijdstippen op de hoogte te houden van de toestand van de data protectie omgeving, inclusief een beknopt overzicht van incidenten en trends daarin. ▪ Het is ook essentieel om een stimulans tot continue verbetering in te bouwen

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Stel een gegevensbeschermings-verklaring op die uitlegt welke gegevens verwerkt worden en op welke manier, en hoe ze beveiligd worden.	Voor (en ten laatste op) het moment van verzameling van de gegevens moet er duidelijke info aan de betrokken persoon geleverd worden
	De data protectie verklaring moet op latere tijdstip door de betrokken persoon te allen tijde kunnen geconsulteerd of opgevraagd worden.
Communicatie procedure voor het uitoefenen van de rechten van betrokkene	De betrokken persoon moet duidelijke uitleg ontvangen hoe hij zijn rechten onder de AVG kan uitoefenen, zoals onder meer recht op informatie, rectificatie, gegevensverwijdering, beperking van verwerking, overdraagbaarheid, bezwaar verwerking en profilering, … waar en indien van toepassing.

4.5 Beheer Activa

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie stelt een inventaris op van haar kernactiva, ongeacht de categorie ervan (informatie, gegevens, transmissie, toepassing, netwerken, processen, systemen etc.).	Elk element van de architectuur zal gedetailleerd worden uitgewerkt in de ontwerpfase ("by design") en alle elementen zullen worden overgenomen om te profiteren van een mapping van de informatie-infrastructuur van de organisatie ("by default").
	Elk onderdeel van deze inventarisatie wordt toegewezen aan een verantwoordelijke persoon (met zijn/haar back-up) wiens contactgegevens worden bijgehouden.
	Voor elk actief worden de toegekende toegangsrechten en machtigingen overgenomen. Toegang en machtigingen worden verleend op “need-to-know/need-to-use"-basis.
	Wanneer de verantwoordelijke een persoon buiten het bedrijf is (softwareleverancier, onderaannemer) worden de referenties van

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	het contract opgenomen in de inventarislijst, alsook de contactgegevens in geval van nood.
	Deze inventarisatie wordt beveiligd maar is bekend bij sleutelfiguren in de organisatie en bij degenen die een incident moeten beheren.
Er zal een inventaris van informatiesystemen worden bijgehouden.	Een inventarisatie van geïnstalleerde systemen en cliënt-diensten (bv. lijst van applicaties en gebruikers van applicaties en gegevens op de server).
	De inventarisatie van de onderlinge afhankelijkheid van systemen op technisch en functioneel niveau zal worden bijgehouden.
	De aanwijzing van de voor het systeem verantwoordelijke persoon of personen en de contactgegevens (intern personeel, leverancier of onderaannemer) worden bijgewerkt.
	Systeemconfiguratie wordt gedocumenteerd.
	De procedures voor back-up, herstel en archivering van het systeem worden up-to-date gehouden.
	Inventaris van connectiviteit en redundantie.
	Productie, wijzigingen, updates en onderhoudsprocedures: versie, change & onderhoudsproces & beveiligingsmaatregelen.
	Procedures voor inloggen en systeem-monitoring.
	Procedures voor de vernietiging/ontmanteling van een essentieel goed.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	Voor elk onderdeel van de infrastructuur worden de beschermingsmiddelen gedetailleerd omschreven en aan één verantwoordelijke persoon toegewezen. Let erop dat je een onderscheid maakt tussen mensen met operationele verantwoordelijkheid en degenen die verantwoordelijk zijn voor ontwikkeling en testen.
Elke organisatie zorgt ervoor dat er een procedure voor het beheer van informatiemiddelen is, waarbij rekening wordt gehouden met het belang van de gegevens van de organisatie.	Er wordt een categorisatie van de informatie gedefinieerd waarbij op zijn minst rekening wordt gehouden met de voor deze informatie vereiste confidentialiteit, integriteit, beschikbaarheid en authenticiteit.
	Er zal een procedure worden gedefinieerd om deze informatie te markeren.
Elke organisatie zal de regels en beveiligingsmaatregelen voor het gebruik van verwijderbare media definiëren.	Er zal een toegangsbeleid vastgelegd worden dat het gebruik van verwijderbare media regelt. Dit zijn niet alleen USB sticks, maar ook CD/DVD, tapes, mobiele harde schijven, geheugenkaarten, enz… , Verder moet dit beleid rekening houden met de data levenscyclus en voor elk van de stappen een voldoende bescherming bieden.
	Er zal een procedure voor de behandeling van verwijderbare media worden gedefinieerd.
	Er zal een procedure voor verspreiding, opslag, archivering en vernietiging van gegevens (beheer van de levenscyclus van gegevens) worden gedefinieerd.
Elke organisatie voert beveiligingsmaatregelen uit voor gevoelige gegevens en informatiesystemen.	Er zullen beveiligingsmaatregelen worden gedefinieerd voor systemen die gebaseerd zijn op de categorisatie van gegevens.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	Definitie van regels en middelen voor confidentialiteit, integriteit en beschikbaarheid van gegevens en informatiesystemen.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
De persoonsgegevens zijn voldoende beschermd op basis van de risico analyse.	Zoals vermeld in AVG artikel 32 , moet de organisatie passende technische en organisatorische maatregelen nemen om de verwerking volgens de regels te laten verlopen.
	Er zijn verschillende categorieën van persoonsgegevens gedefinieerd, op basis waarvan de beschermende maatregelen worden uitgevoerd

4.6 Toegangscontrole

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Unieke toegang: De organisatie zal duidelijke toegangsregels (beveiligingsmaatregelen, RCA-model) per actief (ruime betekenis) definiëren.	In het algemeen, voor toegang tot essentiële activa, moet per persoon een toegangscode worden gebruikt. Het delen van toegangscodes is niet toegestaan.
	De door de organisatie gebruikte niveaus van authenticatie zullen worden gedefinieerd in overeenstemming met de categorisatie van informatie die in de risicoanalyse wordt geïdentificeerd.
De organisatie zal een register van toegangsbevoegdheden bijhouden en bijwerken.	Dit register zal regelmatig worden herzien en bijgewerkt.
	Dit register zal een correct beheer van de toegangsrechten en de controle en actualisering ervan mogelijk maken.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	De machtiging van een verantwoordelijke persoon is vereist op basis van deze verschillende criteria (die door de organisatie moeten worden gedefinieerd: accreditatiedienst, contract).
Gebruikers worden goed opgeleid en geïnformeerd over hun taken en verantwoordelijkheden.	Bijzondere aandacht zal worden besteed aan opleiding en informatie over toegangsmiddelen, met inbegrip van wachtwoorden. (De elementen herhalen voor een sterk wachtwoord, het delen van wachtwoorden vermijden, het wachtwoord niet opschrijven, niet hetzelfde wachtwoord gebruiken voor privé- en professioneel gebruik)
Voor elk onderdeel van de inventarisatie (versterkende beveiligingsmaatregelen, rapportage aan een autoriteit)	Worden de acties gecontroleerd door middel van een logboek, waarvan de toegang beveiligd is en alleen toegankelijk is voor geautoriseerde en geïdentificeerde personen.
	Verdachte handelingen of incidenten worden gerapporteerd en onderzocht en er wordt een onderzoeklogboek bijgehouden om te bepalen of verdere actie nodig is.
	Er wordt een detectiesysteem voor onbevoegde toegang onderhouden
Enkele bijzondere gevallen:	Communicatie-elementen voor netwerk-communicatie zullen deel uitmaken van deze inventaris en worden beschouwd als kritieke elementen van de informatiearchitectuur.
	Een extra element wordt toegevoegd aan de connectiviteit: om de bedrijfscontinuïteit van de organisatie te waarborgen, wordt de connectiviteit verdubbeld
Toegangscontrole op persoonsgegevens	Op basis van de classificatie/categorisatie van de persoonsgegevens moeten er processen en procedures ingericht worden die zorgen dat ▪ Er toegangscontrole is op de gegevens met logboeken

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	▪ Voldoende sterke authenticatie methodes gebruikt worden Medewerkers die het bedrijf verlaten mogen geen toegang meer hebben tot persoonsgegevens in het bedrijf

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Verificatie identiteit van betrokken persoon bij uitoefenen van rechten	Een proces die gepaste identificatie van de betrokken persoon garandeert wanneer de betrokken persoon zijn rechten wenst uit te oefenen zoals voorzien in de AVG. Belangrijke opmerking: Een gebrekkige of verkeerde implementatie kan op zich tot datalekken leiden, dus het is erg belangrijk om hier erg voorzichtig mee om te gaan.

4.7 Cryptografie

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Als er cryptografische maatregelen worden geïmplementeerd, zal de organisatie details geven:	Documentatie van ▪ Categorisatie activa ▪ Type maatregel (data in transport, data in rust, data in executie, …) ▪ Risico niveau ▪ Gebruikte categorie cryptografische maatregel ▪ Type crypto-algoritmes ▪ Geldigheid sleutels en certificaten ▪ …
In het algemeen, voor toegang tot essentiële activa, moet per persoon een toegangscode worden gebruikt. Het delen van toegangscodes is niet toegestaan.	Een beveiligingsmaatregel i.v.m. het gebruik van cryptografie moet ten uitvoer worden gelegd, gevalideerd, gecommuniceerd en gehandhaafd.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Sleutelbeheer	Een procedure wordt gedefinieerd i.v.m. het beheer, de bescherming en de levensduur van cryptografische sleutels.

Veiligheidsmaatregel (AVG)	Minimaal toe te passen maatregelen
Persoonsgegevens worden voldoende beschermd tijdens opslag, transport en gebruik van persoonsgegevens	Zoals beschreven in AVG artikel 32 moeten persoonsgegevens passend beveiligd worden bij opslag, transport en gebruik, bijvoorbeeld door middel van encryptie, pseudonymisering of andere bescherming afhankelijk van de situatie.

4.8 Fysieke en milieuveiligheid

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Beveiligde ruimten	Elke organisatie moet de toegang tot gebouwen en lokalen beperken tot bevoegde personen en moet zowel tijdens als buiten de werktijden controles uitvoeren.
Bescherming van apparaten.	Elke organisatie dient preventieve maatregelen te nemen tegen verlies, schade, diefstal of ongeoorloofde toegang van de activa van de organisatie en tegen onderbreking van de activiteiten van de organisatie.
Clear screen	Gebruik schermbeveiliging en time-outs op schermen om te vermijden dat bij afwezigheid informatie kan gelezen worden
Clear desk beleid	Zorg ervoor dat er geen informatie, papieren en documenten onbewaakt achterblijven op werkplaatsen van de medewerkers

4.9 Operationele veiligheid

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Voor elke asset	Login & monitoring met melding van incidenten en getroffen beveiligingsmaatregelen.
Een inventarisatie van de testomgeving zal worden bijgehouden.	Om de testomgeving duidelijk te scheiden van de productieomgeving, zullen minstens volgende maatregelen uitgevoerd worden: ▪ Machtigingen – Vergunningen. ▪ De logboeken. ▪ Terugvalscenario voor updates en uitwisseling. ▪ Tests & updates uitgevoerd met timing & logboek.
De minimale technische maatregelen die voor de architectuur worden genomen, zijn:	▪ Anti-malware/antivirus moet up-to-date zijn. ▪ Detectiesysteem voor inbraak of onbevoegde of niet-toegelaten software. ▪ Procedures voor het blokkeren/isoleren van anomalieën/niet-geautoriseerde toegang. ▪ Up-to-date hardware & software met pre-testen van nieuwe releases en fall-back-scenario's. ▪ Incidentmanagement (inclusief communicatie). ▪ Beschikken over back-upprocedures: maken, testen van restauratie. ▪ Beschikken over een procedure met betrekking tot gegevensencryptie.

4.10 Communicatiebeveiliging

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Bij een beveiligingsmaatregel moet rekening worden gehouden met de beveiliging van de informatieoverdracht om ongeoorloofde toegang tot de infrastructuur en gegevens van de organisatie te voorkomen, ongeacht of deze toegang al dan niet vrijwillig is.	Een gedetailleerd en goed onderhouden systeem beheren, controleren, toegangscontroles uitvoeren, zowel fysiek als logisch.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Deze beveiligingsmaatregel dient rekening te houden met de toegankelijkheid die nodig is voor de systemen van de organisatie.	Een inventarisatie maken van de stromen, de beheerders ervan en de verleende toegang.

4.11 Aankoop, ontwikkeling en onderhoud van informatiesystemen

Veiligheidsmaatregel	Minimaal toe te passen maatregels
Stel voor alle informatiesystemen controles in voor acquisitie, ontwikkeling en onderhoud. Er zal bijzondere aandacht worden besteed aan outsourcing, gebruik van cloud-services of aankoop van producten.	In elk nieuw project moet beveiliging deel uitmaken van elke stap. Er moet een gestructureerde aanpak worden ontwikkeld, onder toezicht van een organisatiemanager, om de integratie, de ontwikkeling, het onderhoud en de ontmanteling van de door de organisatie gekozen oplossingen effectief te beheren. De organisatie zal een inventarisatie maken van de geselecteerde systemen en de verwijzing naar contracten en verplichtingen (SLA, NDA) om de monitoring en het beheer van uitbestede oplossingen te verzekeren.
Daarnaast houdt elke organisatie een logboek bij met de volgende gegevens:	• Wijzigingen. • Incidenten en de gevolgen ervan. • De toegangen. • Het onderhoud. • ingevoerde beveiligingsmaatregelen.
In het logboek zullen ook de beveiligingsmaatregelen worden vermeld waarvoor de nodige maatregelen zijn getroffen:	• Continuïteitsmaatregelen. • Integriteit van de gegevens. • Confidentialiteitsprobleem. • Beschikbaarheid van het systeem. • Incidentele beheersmaatregelen.
De organisatie zal procedures implementeren om haar oplossingen up-to-date te houden en te zorgen voor een geteste back-up-beveiligingsmaatregel voor zowel haar systemen als gegevens.	

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Bij aankoop, ontwikkeling en onderhoud van systemen moet er processen en procedures gebruikt worden die persoonsgegevens beschermen, zowel bij ontwerp als operationeel beheer	Ref AVG Art 25. Opzetten en onderhouden van processen en procedures die ervoor zorgen dat • Systemen en Processen veilig ontworpen worden • Systemen en processen veilig gebruikt worden (gegevensbescherming door standaard instellingen)

4.12 Betrekkingen met derden (leveranciers, autoriteiten)

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
De organisatie zorgt ervoor dat de contracten tussen de partijen beveiligingsmaatregelen bevatten, opgelegd door de organisatie op door wet- en regelgeving (inclusief het AVG, Cyber Act) en de elementen van controle en toetsing bevatten.	
Elke organisatie zorgt ervoor dat bij gebruik van cloud-computing-diensten de nodige beveiligingsmaatregelen worden ingezet die nodig zijn voor de organisatie.	Bepaal de vereiste beschermingsmaatregelen op basis van een risicoanalyse van de uitbestede diensten/data. Hiervoor kan je bv. gebruikmaken van de beschikbare auditrapporten, zoals ISO27001, ISAE3402, ENISA, WITHOUT, CSA, … etc. Valideer auditrapporten en certificeringen van cloud-dienstverleners.
	Zorg dat het recht op audit opgenomen is de afspraken en contracten met derden.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie zal erop toezien de relaties met leveranciers en met de autoriteiten te definiëren.	In contracten/documenten moet duidelijk worden vastgelegd wat **wie de verwerkings-verantwoordelijke is en welke partij verwerker is** en hoe verantwoordelijkheden verdeeld worden. Deze overeenkomst minstent de elementen bevatten zoals opgesomd in artikel 28 AVG.
	Zoals aangegeven in AVG Art. 28.3, moet er met elke verwerker duidelijk afgesproken worden hoe de data protectie operationeel geregeld wordt, inclusief vereiste beveiliging en gedrag, incidentbeheer, melding van inbreuken, contact met autoriteiten (of niet)

4.13 Gecoördineerd bekendmakingsbeleid van kwetsbaarheden (CVDP)

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Gecoördineerd bekendmakingsbeleid van kwetsbaarheden, hieronder CVDP genoemd (*Coordinated Vulnerability Disclosure Policy*, EN). Elke organisatie stelt een CVDP op en onderhoudt het plan.	Laat het beleid goedkeuren door iemand die jouw organisatie rechtsgeldig kan vertegenwoordigen (bv. de directeur). Het CVDP is een **verzameling regels** die op voorhand zijn vastgelegd door de organisatie, verantwoordelijk voor de ICT, en **die veiligheidsonderzoekers** (ethische hackers) of het grote publiek binnen de wettelijke grenzen toelaten om **met goede bedoelingen potentiële kwetsbaarheden** in de systemen van die organisatie te zoeken of haar alle relevante informatie door te geven die ze hieromtrent ontdekken, zonder hiervoor vervolgd te worden.
	De inhoud van het CVDP moet **op jouw website beschikbaar** zijn en **toegankelijk voor de derden.** Indien mogelijk moet het CVDP in de verschillende talen van jouw website zijn opgesteld. We raden aan een beknopte maar volledige tekst op te stellen, met duidelijke vermelding van: • Het toepassingsgebied van jouw beleid. • De grenzen van het toegangsrecht.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	• De mate waarin de ethische hacker informaticagegevens mag wijzigen of verwijderen, of niet.
Zowel voor interne als externe medewerkers en betrokken personen moet er een procedure bestaan die het mogelijk maakt om verdachte activiteiten te rapporteren	Een procedure om mogelijke of vermoedelijke inbreuken te rapporteren, te registeren en te behandelen zodat kwetsbaarheden voortijdig en gestructureerd kunnen behandeld worden.

Mesure de sécurité	Mesures minimales à mettre en place
Kennisgeving aan de toezichthoudende autoriteit van een inbreuk op persoonsgegevens	De gegevensbeschermingsautoriteit (GBA) ontvangt binnen 72 uur na de kennisgeving de melding van inbreuken op de beveiliging van persoonsgegevens

4.14 Incident management

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie zet een Incident Management Plan op dat onder meer de volgende taken en verantwoordelijkheden omvat.	Bepalen van rollen en verantwoordelijkheden
	Intern incidentregister dat alle gerapporteerde informatiebeveiligings-incidenten bevat
	Opsporingshulpmiddelen (intern of extern).
	Kennisgeving door een werknemer of derde van indringing, verdachte elementen, verlies of vernietiging etc.
	Waarschuwingsniveaus - definitie van criteria voor escalatie naar een crisis.
	De crisisbeheersingsprocedure (inclusief communicatie).
	Deze procedures moeten aan het personeel worden meegedeeld en er zijn beproefde

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	informatie en opleidingen nodig via verschillende kanalen.
	Gekoppeld aan de IC- & OES-infrastructuren van CERT.be (intelligenceverzameling/uitwisseling van informatie).
	Overeenkomstig andere wettelijke en/of sectorale verplichtingen (bv. op het gebied van energie, bankwezen, telecommunicatie etc.).
Elk incident zal worden geanalyseerd om de relevantie van nieuwe beveiligings-maatregelen te evalueren.	De lessen die uit elk incident (intern en/of extern) worden getrokken, zullen leiden tot een verbetering van de incidentmanagement-procedure voor de organisatie.
	Rapporteren van mogelijke beveiligings-incidenten moet mogelijk gemaakt worden, zonder dat medewerkers hiervoor afgestraft worden of zich blootstellen aan wraakacties van medewerkers of hiërarchische oversten.

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie zet een Incident Management Plan op dat onder meer de volgende taken en verantwoordelijkheden omvat die de behandeling van inbreuken op persoonsgegevens regelt	Bepalen van rollen en verantwoordelijkheden bij het behandelen van incidenten en inbreuken op persoonsgegevens
	Incident register dat alle gerapporteerde informatiebeveiligings-incidenten bevat, met de nodige kwalificatie of deze incidenten moeten gerapporteerd worden aan de bevoegde autoriteiten (GBA)
	Voorzien van opsporingshulpmiddelen (intern of extern).
	Communicatieplan met betrokken partijen - Melding management - Meldig aan autoriteit

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
	- Melding betrokken personen (indien noodzakelijk) - Communicatie met eventuele verwerker of verwerkingsverantwoordelijke
Kennisgeving aan de toezichthoudende autoriteit van een inbreuk op persoonsgegevens	Elke organisatie meldt incidenten in verband met persoonsgegevens overeenkomstig de bepalingen van de artikel 33 en 34 AVG.

4.15 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Voor kritieke systemen of gevoelige gegevens die nodig zijn voor de continuïteit van de organisatie wordt een continuïteitsplan opgesteld, waarbij bijzondere aandacht wordt besteed aan de volgende punten:	Inventaris van kritieke systemen/kritieke activa • Risicobeheer, • Competentie van medewerkers verantwoordelijk voor de verschillende processen/activa die essentieel zijn voor de organisatie, • Benodigde kritieke niveaus voor activering van het continuïteitsplan, • Prioritering van essentiële activa bij het herstel ervan, • Communicatiemanagement, • Crisis communicatie
Onderhoud van het continuïteitsplan.	Een herziening en aanpassing van dit continuïteitsplan zijn noodzakelijk, evenals een test/simulatie.
Beschermingssysteem dat de confidentialiteit, integriteit en beschikbaarheid van de bedrijfs- en persoonsgegevens garandeert	De verwerkingsverantwoordelijk moet er voor te zorgen dat de beschikbaarheid van en toegang tot bedrijfs- en persoonsgegevens na een fysiek of technisch incident tijdig kan hersteld worden
	Bescherming van bedrijfs- en persoonsgegevens tegen verlies, ongeoorloofde wijziging of vernietiging, hetzij door ongeluk of moedwillige acties.

4.16 Naleving en opvolging wet- en regelgeving

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Naleving van wet- en regelgeving.	Elke organisatie handelt in overeenstemming met de wettelijke vereisten en voorschriften.
Elke organisatie zal erop toezien de relaties met leveranciers en met de autoriteiten te definiëren.	In contracten/documenten moet duidelijk worden vastgelegd wat de verantwoordelijkheden van de verschillende betrokken partijen zijn en hoe verantwoordelijkheden verdeeld worden

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Opvolging van wetgeving en advies die door de betrokken autoriteiten worden uitgevaardigd of aangepast.	**Opvolging van publicaties van adviezen en wetgeving van relevante autoriteiten**
	Aanstelling van verantwoordelijke om opvolging te garanderen
	Verwerkersovereenkomst in de zin van artikel 28 AVG.

4.17 Evaluatie en controle van de beveiligingsmaatregelen

Veiligheidsmaatregel	Minimaal toe te passen maatregelen
Elke organisatie organiseert op geregelde tijdstippen een evaluatie van de maatregelen	Een interne of externe evaluatie van de informatiebeveiliging. Deze externe evaluatie kan uitgevoerd worden door de Federale Overheidsdienst voor Interne Audit (FIA).
	Een controleverslag over de veiligheidssituatie van een interne controle of CISO zal worden voorgelegd aan de Raad van Bestuur.
	Een evaluatie of opvolging kan op geregelde tijdstippen uitgevoerd worden, maar het is ook interessant om opvolging uit te voeren, direct na een incident, omdat dit een handige indicator is om een verbeterpunt te realiseren.

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

5 Jaarlijks nazicht van het beveiligingsplan in overleg met het management

Het is aangeraden om dit veiligheidsplan minstens jaarlijks met het management door te nemen.

Dit stelt je in staat het te corrigeren, aan te vullen en het top management bewust te maken van het belang van informatiebeveiliging en gegevensbescherming.

Het informatiebeveiligingsplan moet mettertijd evolueren. Het kan met name worden herzien om rekening te houden met:

- veranderingen in bedreigingen en feedback als gevolg van incidentenbehandeling;
- de resultaten van risicoanalyses en acties naar aanleiding van controles of audits;
- veranderingen in organisatorische, juridische, regelgevende en technologische contexten.

Deze ontwikkelingen worden opgevolgd door het management van de verschillende FOD's, met de volgende hoofdtaken:

- toezicht op de uitvoering van veiligheidsplannen;
- meten van de voortgang en de beveiligingsstatus van jouw organisatie;
- voorstellen van updates;
- voorstellen van aanvullende documenten en richtsnoeren om de tenuitvoerlegging ervan te vergemakkelijken of te verduidelijken;
- opvolging van de evolutie van de technische documenten.

Sommige organisaties zijn verplicht te rapporteren over de status van hun beveiligingsplan en het gegevensbeschermingsplan (zie ISO 29100 en ISO29101).

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

6 Expert Panel

Dit document is tot stand gekomen met de gewaardeerde hulp van medewerkers, security experts en veiligheidsadviseurs van de volgende instanties.

Instantie
FOD Justitie
DGCC
Federale Politie
FOD Kanselarij
FOD Gezondheid
FOD Economie
CCB
FOD BOSA
GBA

7 Acroniemen & Afkortingen

7.1 Terminologie (Algemeen)

Acroniem	Beschrijving
Informatietechnici	Kan worden gedefinieerd als iedereen die, in het kader van zijn verantwoordelijkheden voor een ICT-systeem, toegangsrechten heeft die verder gaan dan het functioneel gebruik van gegevens. Deze omvatten ontwikkelaars, systeembeheerders en beheerders, datamanagers, softwareontwikkelaars en -managers, netwerkexploitanten, consultants en onderaannemers.
Informatiebeveiligingsadviseur	Ondersteund door verwerkingsverantwoordelijke, bevordert de naleving van de wet- en regelgeving over computer-beveiliging. Hij heeft een raadgevende taak en zorgt voor stimulatie, documentatie, controle en bevordering van de navolging van de veiligheidsvoorschriften die worden opgelegd door een wettelijke of reglementaire bepaling. Het bevordert de goedkeuring door personen werkzaam in de organisatie van het gedrag van de veiligheid. In deze context is het duidelijk een bevoorrechte partner van vele mensen in de organisatie die informatie beheren, bijvoorbeeld de eigenaar van de gegevens, de eigenaren van de ondernemingen, maar ook van een heleboel externe partners, leveranciers, de overheid etc.
Verwerkingsverantwoordelijke (BSG, algemeen)	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van bedrijfsgegevens vaststelt;
Actief/Asset	Een actief is een materieel of immaterieel object of kenmerk dat waardevol is voor een organisatie. Er zijn verschillende soorten activa. Sommigen van hen omvatten voor de hand liggende dingen zoals machines, installaties, patenten en software. Maar de term kan ook minder voor de hand liggende zaken bevatten, zoals services, informatie en mensen, en functies zoals reputatie en imago of vaardigheden en kennis.
Informatie-asset	Informatie die waardevol is voor een organisatie.

OPGELET

In de BSG wordt deze term "verwerkingsverantwoordelijke" breder toegepast dan enkel AVG, want het gaat over bedrijfsgegevens EN persoonsgegevens.

(zie verder)

7.2 Terminologie (AVG)

Acroniem	Ref. AVG	Beschrijving
Persoonsgegevens	Art. 4 1)	"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"
Gegevensverwerking	Art. 4 2)	"een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens; "
inbreuk in verband met persoonsgegevens	Art. 4 12)	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot • het verlies, • de wijziging, • de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
Verwerkingsverantwoordelijke onder AVG	Art. 4 7)	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of

		samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

7.3 Afkortingen

Acroniem	Beschrijving
AVG	Algemene Verordening Gegevensbescherming =GDPR (EN)
BCP	Bedrijfscontinuïteitsplan
CIA (EN)	confidentiality, integrity en availability = CIB (NL)
CIB	confidentialiteit, integriteit en beschikbaarheid = CIA (EN)
CISO (EN)	Chief Information Security Officer
GBBK	Gecoördineerd bekendmakingsbeleid van kwetsbaarheden (GBBK) Zie CVDP
GDPR (EN)	General Data Protection Regulation Zie AVG
CVDP (EN)	Coordinated Vulnerability Disclosure Policy (EN)
ADCC	Algemene Directie Crisiscentrum
PDCA (EN)	Plan, Do, Check, Act
CCB	Centrum voor Cybersecurity
GBA	Gegevensbeschermingsautoriteit

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

8 Referenties

Referentie	Beschrijving & URL
AVG	*VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

CENTRUM VOOR
CYBER SECURITY BELGIUM
Wetstraat 18 – Brussels

De verschafte informatie:

* is algemene informatie die geen rekening houdt met specifieke situaties;

* is niet noodzakelijk exhaustief, exact of up-to-date op alle punten.

Verantwoordelijke uitgever:

CENTRUM VOOR CYBERSECURITY België

Wetstraat 16

1000 Brussel